PLAN REGIONAL DE CYBERSECURITE

2023 - 2025

Table des matières

Contexte et enjeux de la cybersécurité

La cybersécurité se définit comme l'état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace, susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.

Notre économie, et plus largement notre société, intègrent désormais nativement les usages du numérique pour leurs apports en matière d'accès à l'information, de transmission, de traitement de données et d'interconnexion des réseaux de données.

En corollaire, les systèmes d'informations, qui concentrent ainsi une part croissante du patrimoine de chaque personne physique ou morale, deviennent un enjeu de maîtrise informationnelle : toute perte de contrôle sur son système d'information expose à un risque élevé de perte, de vol, de piratage ou de destruction de données.

La sécurisation des systèmes d'information est devenue une condition *sine qua non* de l'établissement de la confiance numérique, de la stabilité des acteurs institutionnels, de la protection des citoyens et du développement de notre économie et de notre société.

Le sujet est complexe dans la mesure où il relève de technologies de plus en plus sophistiquées mais également de la prise de conscience collective et individuelle, comme de l'évolution des comportements induits

Si la notion de sécurisation des systèmes d'information était dans les années 2000 l'apanage des acteurs étatiques dans une approche de cyberguerre et de cyberespionnage, on observe, depuis une décennie, l'émergence d'une cybercriminalité organisée et professionnalisée qui aborde le piratage de données comme une entreprise économique.

A travers des attaques plus ou moins automatisées, ciblées ou aléatoires, les cybercriminels cherchent à prendre le contrôle partiel ou total d'un système d'information. Le gain financier est obtenu par la vente de données et/ou le rançonnage.

A cela s'ajoutent des attaques plus stratégiques, de la part d'acteurs idéologiques ou étatiques, destinées bien souvent à affaiblir les Etats, collectivités territoriales, services publics et entreprises de tout taille, qui en sont la cible. Les motivations sont variées, parfois combinées : espionnage, perturbation ou neutralisation des services essentiels, influence, atteinte à la crédibilité d'un Etat, d'un gouvernement, d'un dirigeant ou d'une grande entreprise nationale.

La surface d'exposition des entreprises et des organisations aux cyberattaques s'est considérablement augmentée sous l'effet de plusieurs facteurs :

- La pandémie, qui a fortement accéléré le télétravail, multipliant les connexions distancielles avec les systèmes d'informations des entreprises.
- La transformation numérique des entreprises qui se poursuit, caractérisée notamment par un usage de plus en plus fort des services en ligne et par l'interconnexion des systèmes d'information des entreprises avec leurs écosystèmes (services cloud, sites satellites délocalisés, sous-traitants, supply chain, clients, …).
- L'adoption de nouvelles technologies comme l'Internet des objets (IoT) qui accroissent très fortement le nombre de capteurs qui produisent de la donnée numérique et qui se connectent avec les systèmes d'information à sécuriser.
- Les progrès de l'intelligence artificielle, qui multiplient les échanges de données mais qui est également utilisée par les cyberattaquants pour améliorer leurs outils.
- La connexion du système d'information de gouvernance (IT) avec le système de production numérisé (OT) de l'entreprise industrielle.

L'ANSSI[1], autorité nationale en matière de cybersécurité rattachée aux services du Premier ministre, observe ainsi une **multiplication par 8 des attaques entre 2021 et 2022**, après une multiplication **par 4 entre 2020 et 2021**. La médiatisation des cas d'attaques s'accélère alors même que la plupart des victimes ne souhaitent pas communiquer par peur des effets sur leur image.

Malgré la difficulté à identifier l'ensemble des attaques contre des organismes publics ou privés en France, les experts s'accordent sur le fait que personne n'est épargné : la taille ou l'activité des structures n'est pas prise en compte par les attaquants.

Face à cette menace, on observe un très faible niveau de maturité des TPE et des PME en matière de cybersécurité, décorrélé d'une digitalisation qui s'accélère. Selon l'IFOP et Xerfi en novembre 2021, **75% des chefs d'entreprise français** de PME/TPE estimaient avoir un **risque faible d'être touché par une cyberattaque** et **80%** considéraient leur **entreprise bien protégée contre ces risques**.

Pour tenir compte de ces différentes évolutions, la France a actualisé en février 2021 sa stratégie en matière de cybersécurité, en cohérence avec les politiques européennes. Cette stratégie repose sur 4 axes complémentaires :

- **Soutenir la demande de cybersécurité** en renforçant la prise de conscience de la population au risque cyber via des actions de sensibilisation et de mise en valeur de l'offre française de cybersécurité :
    - En faisant du Forum International de la Cybersécurité de Lille un événement de référence mondial ;

[1] Agence Nationale de la Sécurité des Systèmes d'Informations.

- En déployant des projets portés par l'ANSSI visant à renforcer la sécurité numérique de l'Etat et des territoires, pour un budget total de **136 millions d'euros**, à travers notamment :
  - Un **parcours d'accompagnement** à la cybersécurité pour les collectivités
  - un projet industriel global de **démonstrateurs**,
  - le déploiement de **Centres Régionaux de réponse d'urgence aux victimes d'incidents cyber** (CSIRT) pour compléter l'assistance directe de l'ANSSI aux Opérateurs de Services Essentiels et Organismes d'Intérêt Vitaux (réseaux de distribution et de transport, périmètres sensibles des CHU, …) et l'aide en ligne du portail Cybermalveillance aux particuliers et très petites structures ;

- **Développer des solutions souveraines et innovantes de cybersécurité**, aux côtés des acteurs privés, en soutenant la recherche et l'innovation :
  - L'Etat co-investira dans l'écosystème notamment par la création d'un **incubateur de startups de cybersécurité** ;
  - Le CEA, le CNRS et l'INRIA ont été mandatés pour piloter **un programme de recherche doté de 65 millions d'euros**, dont l'objectif est de maîtriser l'ensemble des technologies clés nécessaires pour disposer d'une capacité complète et souveraine pour prévenir les menaces ;
  - Un **objectif de 500 millions d'euros de fonds publics et privés** pour le développement de **solutions innovantes et souveraines** est attendu d'ici 2025.

- **Renforcer les liens et synergies entre les acteurs de la filière** en fédérant l'écosystème de la cybersécurité en France par la mise en place d'un lieu « totem », le **Campus Cyber** à Paris - La Défense et en encourageant la déclinaison en Campus Cyber Territoriaux. Ce rapprochement doit favoriser des projets communs de partage de données et l'émergence de solutions globales souveraines aptes à concurrencer l'offre mondiale.

- **Former les jeunes et les professionnels** aux métiers de la cybersécurité
  - En s'appuyant sur un meilleur diagnostic des métiers et formations existantes et en adaptant les formations à tous les niveaux pour répondre aux besoins en compétences ;
  - Par un renforcement de la recherche en cybersécurité (masters spécialisés, augmentation des doctorants et thèses CIFRE, …).

Au niveau européen, la stratégie a été consolidée en décembre 2020 pour **renforcer la résilience de l'Europe face aux cybermenaces**. Elle comprend :

- Le déploiement d'instruments de réglementation, d'investissement et d'action, au travers du **programme Horizon Europe**.

- L'engagement à **investir 1,6 milliard d'euros dans la capacité de réaction en matière de cybersécurité** et le **déploiement à grande échelle d'infrastructures et d'outils** de cybersécurité dans l'ensemble de l'UE dans le cadre du programme pour une **Europe numérique pour la période 2021-2027**,

- La création d'un **Centre européen de compétences industrielles, technologiques et de recherche** en matière de cybersécurité.

L'Etat et l'Europe sont alignés dans la **nécessité de structurer et développer la filière des solutions de cybersécurité** pour

- appréhender les enjeux de souveraineté,
- prendre une part significative du marché mondial de la cybersécurité évaluée, selon les sources, entre **140 et 217 milliards d'euros en 2021**, avec des projections entre **480 et 530 milliards d'euros en 2030**.

L'État a identifié le **niveau régional** comme le plus pertinent pour garantir une bonne **mise en œuvre des initiatives nationales** et une **adaptation aux contextes et spécificités** de chaque territoire pour les **TPE, PME, Entreprises de Taille Intermédiaire** et les **collectivités territoriales de taille petite et moyenne**.

Les **Grandes Entreprises et collectivités de grande taille** disposent de **ressources propres** ou sont **prises directement en charge par l'ANSSI**.

Les **particuliers** et les **TPE et collectivités sans système d'information** relèvent prioritairement de l'action d'**ACYMA**, un Groupement d'Intérêts Publics mis en place par l'Etat pour la sensibilisation au risque numérique, à l'assistance aux victimes de cyberattaques et à l'observation de la menace cyber pour ces populations. Il agit essentiellement à travers le portail **Cybermalveillance** qui propose des **ressources documentaires** et des **services en ligne**.

Cadre du plan régional de cybersécurité

Pour la Région Grand Est, le numérique constitue un enjeu fort et transverse qui traverse plusieurs ambitions :

- un territoire connecté et attractif
- un territoire de confiance et responsable
- une économie régionale résiliente, compétitive et proactive dans ses transformations
- une filière régionale numérique compétitive et conquérante
- une décision publique appuyée par la donnée
- une capacité de R&D et de formation à même de répondre aux besoins actuels et futurs du territoire

Des actions ambitieuses ont déjà été initiées telles que le **plan Très Haut Débit**, qui a permis de déployer la fibre jusqu'à l'abonné sur l'ensemble du territoire régional fin 2022, le **lycée 4.0** qui remplace les manuels par des ressources numériques et équipe l'ensemble des lycéens

en ordinateurs ou tablettes, et les programmes orientés entreprises comme le plan **Industrie du futur** et **Ferme du futur** qui accompagnent la transformation numérique de nos écosystèmes industriels et agricoles ou le programme **Transformation Digitale Grand Est** qui visent la digitalisation de centaines de petites entreprises agricoles, artisanales, commerçantes ou du tourisme.
Le **plan régional Intelligence Artificielle**, lancé en 2019 avec une approche 360°, a fait de cette technologie numérique de rupture une priorité de développement économique.

La transformation numérique de notre économie et de notre territoire est donc au cœur des priorités régionales, comme l'a rappelé le Business Act Grand Est en en faisant un des trois leviers de transition régionale.
A l'échelon régional, cette transformation numérique ne pourra durablement se développer sans une maîtrise du risque cyber propre à chaque acteur économique ou territorial.

La **structuration de la filière numérique**, et en son sein de la filière Cybersécurité, est un axe essentiel de cette stratégie régionale. Elle se met en œuvre au travers du **Grand Est Transformation (GET) Numérique** initié par le volet 2 du Business Act Grand Est. Pour mémoire, le Business Act Grand Est a pour objectif d'accélérer la transformation des entreprises régionales à l'aulne de 4 axes du changement dont celui de la transformation numérique. A ce titre, il s'appuie sur 2 piliers que sont d'une part le parcours de transformation des entreprises et par ailleurs les GET, véritable centre de ressources et d'expertises ; l'objectif étant de favoriser un circuit court entre la demande et l'offre régionale et en rebond le développement de la valeur ajoutée régionale.

Ainsi, elle vise un double objectif :

- **Répondre aux besoins de nos entreprises régionales** par une offre régionale de solutions numériques, compétitives et innovantes
- **Développer la part de la filière régionale du marché numérique national, européen et mondial**, très dynamique et pourvoyeur d'emplois qualifiés.

Le GET numérique est un centre de ressources et d'expertise dont la Région a confié l'animation à l'agence Grand Enov+. Il a pour objectifs de :

- **Structurer et renforcer une offre numérique mature et innovante**, au meilleur état de l'art ;
- **Accompagner les offreurs de solutions innovants du Grand Est dans leur développement** :
    - Commercial
    - Technologique
    - Organisationnel
    - Financier

Par offreur de solution, on entend un acteur économique régional proposant une offre de produits et/ou de services sur une thématique numérique, ici la cybersécurité.

Pour atteindre ces objectifs, le GET numérique a pour missions de :

- **Structurer et coordonner des communautés thématiques** d'offreurs, y compris les forces académiques et les organismes de formation (voir figure 1). **Sept communautés**, appelées DAS[2], ont été identifiées :
  - Data / Intelligence artificielle,
  - Cybersécurité,
  - Cloud,
  - Numérique responsable
  - Technologies émergentes (dont quantique, xG, Web 3 …),
  - Technologies immersives (réalité virtuelle / réalité augmentée),
  - Modernisation des infrastructures et usages numériques;

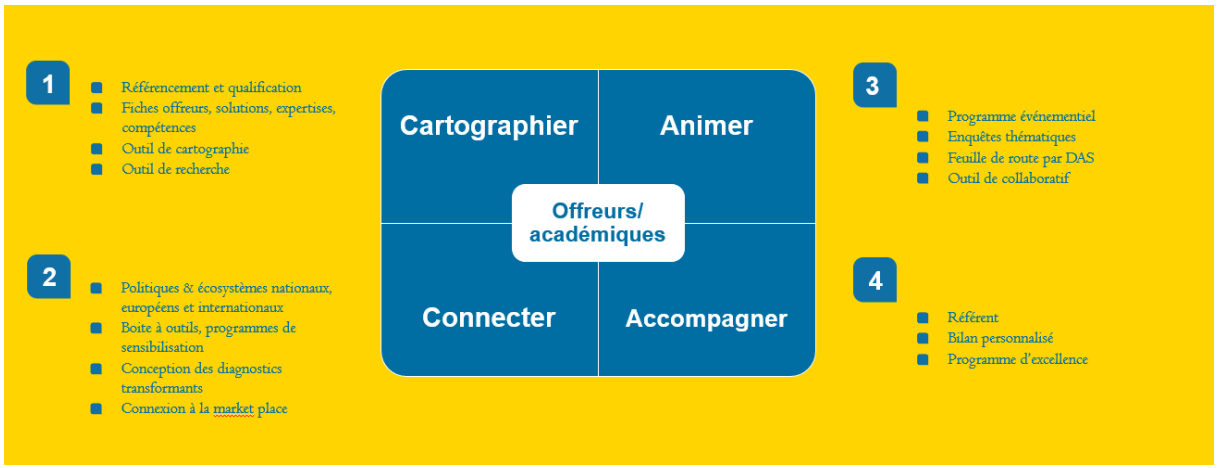

Figure 1 structuration des communautés du GET Numérique

- **Contribuer à la transformation des entreprises** et organisations du territoire, en appui des parcours régionaux d'accompagnement de la Région (voir figure 2) ;

[2] Domaine d'Activité Stratégique

Figure 2 contribution des DAS au parcours régional d'accompagnement

- **Anticiper les besoins en compétences clés** et faciliter l'accès aux talents ;
- **Faire rayonner** les offreurs régionaux et **attirer** de nouveaux offreurs et des talents
- Promouvoir un **numérique responsable.**

Le GET Numérique a été lancé le 24 mars 2022 à Troyes. Depuis, 5 DAS ont été lancés : **Intelligence artificielle** (130 acteurs régionaux référencés), **Cybersécurité** (80 acteurs régionaux référencés), **Numérique responsable, Technologies immersives** et **Cloud**; Le DAS **Technologies émergentes**, par sa nature plus prospective et multisectorielle, se structurera différemment mais des travaux sur le quantique sont déjà lancés.

La cybersécurité s'impose comme une priorité compte tenu de l'empreinte numérique exponentielle du territoire et de la nécessité de pouvoir s'appuyer sur des solutions, idéalement souveraines, afin de garantir la maitrise de la donnée de bout en bout.
Cette feuille de route complète celle déjà lancée en 2019 sous la forme du Plan Régional IA. Ces feuilles de route thématiques sont reprises dans les travaux de réactualisation du Schéma Régional de Développement Economique, d'Innovation et d'Internationalisation (SRDEII).

De même, cette démarche en faveur de la cybersécurité est développée en lien avec la Stratégie de Spécialisation Intelligente (S3).

Présentation du Plan régional de cybersécurité

A travers ce plan, **l'ambition** est la suivante **: devenir un territoire de confiance, où l'ensemble des organisations publiques et privées peuvent profiter des bénéfices du numérique, en maîtrisant les risques sur leurs systèmes d'information, en s'appuyant notamment sur des forces académiques et des offreurs de solutions régionaux à l'état de l'art.**

Au-delà de la nécessité d'une coopération réussie avec les autorités nationales en cybersécurité, l'**ambition est d'inscrire la Région Grand Est dans une approche multilatérale de la cybersécurité (Allemagne, Suisse, Luxembourg, Belgique) afin de répondre aux besoins d'un territoire et d'une économie transfrontaliers de plus en plus intégrés.**

Voici les principaux objectifs de la stratégie régionale :

- Contribuer à la sécurité et la fiabilité des acteurs régionaux dans une logique de transformation ;
- Maintenir la recherche et l'innovation en cybersécurité (notamment auprès des offreurs de solutions) au meilleur état de l'art mondial ;
- Assurer en quantité et en qualité le développement des compétences nécessaires ;
- Fédérer tous les acteurs, afin d'en faire une communauté forte, dans une double logique de coopération et de visibilité/attractivité ;

Le plan proposé s'articule autour du processus de sécurisation des organisations régionales face aux cybermenaces (voir figure 3).

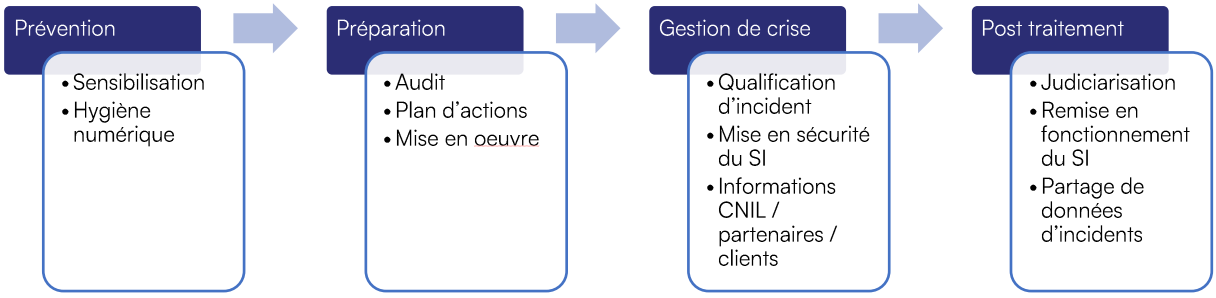

Figure 3 Processus de sécurisation des organisations face aux cybermenaces

1) **Prévenir les cybermenaces** par une **sensibilisation des dirigeants** de l'organisation aux enjeux du risque Cyber et à son caractère systémique ;
2) **Préparer l'organisation** aux cybermenaces en **accroissant son niveau de résilience en cybersécurité :** par un soutien à l'évaluation du niveau de cybermaturité, par la définition de plans de remédiation et par la mise en œuvre de projet d'amélioration de la cybersécurité dans l'organisation ;

3) **Accompagner la gestion de la crise cyber** par une qualification précise de l'incident, par la mise en sécurité du système d'information et par l'information réglementaire de la CNIL, des partenaires et clients si nécessaire.
4) **Soutenir la sortie de crise cyber** par la remise en fonctionnement du système d'information, par l'aide au dépôt de plainte et par le partage de données relative à l'incident pour réduire le risque de propagation.

A ce processus de cybersécurité des organisations, qui va structurer l'action régionale, s'ajoutent 2 thématiques transverses qui impactent l'ensemble du processus (voir figure 4) :

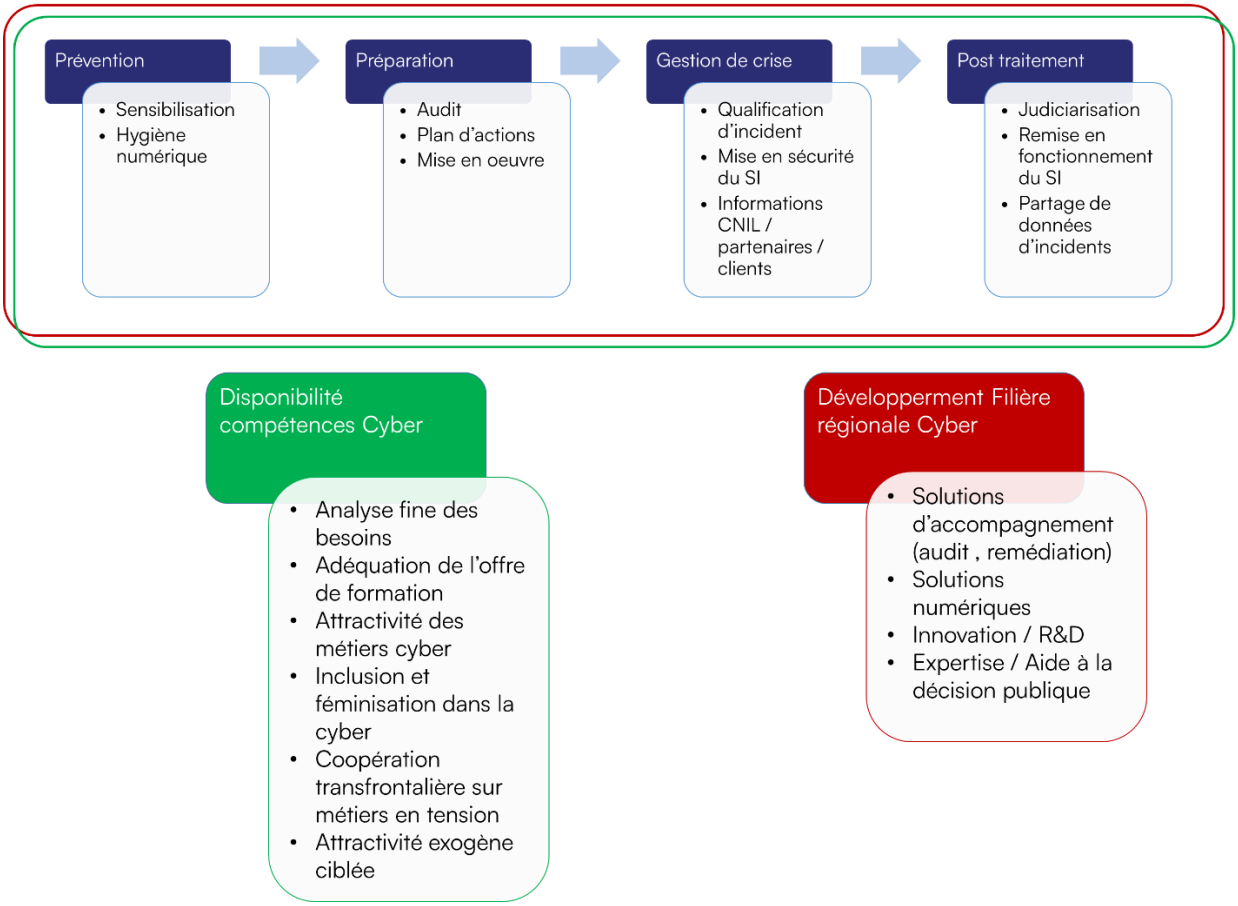

Figure 4 Structuration de l'action régionale pour la cybersécurité des organisations

5) **Animer et développer la filière régionale de la cybersécurité,** en développant les partenariats vertueux entre la recherche, les forces académiques et les offreurs, tout en bénéficiant de la dynamique d'un marché mondial de la cybersécurité en forte croissance ;
6) **Développer les compétences en cybersécurité** pour répondre aux besoins croissants des entreprises et de la filière, par la mise en place de formations initiales et continues au niveau régional et par des actions d'orientation et promotion ciblées sur les publics jeunes et féminins pour valoriser les métiers de la cybersécurité ;

Face à une menace systémique et commune à l'ensemble des acteurs régionaux, la mise en œuvre de ce plan régional doit être fédérative pour favoriser **les collaborations,** optimiser et **mutualiser des ressources rares et coordonner les initiatives** de terrain**.** Le projet de **Campus Cyber Grand Est** offre cette opportunité de fédération de l'écosystème régional**.** C'est l'objet d'un septième point du plan régional de cybersécurité.

1. Prévenir les cybermenaces par la sensibilisation de tous les acteurs régionaux

La nature des cyberattaques et la diversité des victimes confirment le caractère systémique des cybermenaces sur le territoire régional : plus aucun acteur, collectivité, association, particulier ou entreprise, n'est épargné. Cet état de fait n'est cependant pas encore partagé par tous et la gestion du risque cyber doit commencer par la mobilisation de tous les acteurs de la région.

La Région Grand Est entend faire de cette mobilisation contre les cybermenaces une grande cause régionale pour les prochaines années.

Cette mobilisation passe par une sensibilisation à la cybersécurité des différentes catégories d'acteurs régionaux.

La sensibilisation des particuliers et très petits acteurs publics ou privés

Par très petits acteurs publics ou privés, on entend des acteurs sans réel système d'information structuré : un poste de travail unique et des usages proches des usages des particuliers.

Cette catégorie d'acteurs bénéficie déjà des ressources et services proposés par Cybermalveillance[3], le site internet du gouvernement dédié à la sensibilisation au risque numérique, à l'assistance aux victimes de cyberattaques et à l'observation de la menace cyber pour ces populations.

Le GIP ACYMA, opérateur public-privé de la plateforme Cybermalveillance, ne dispose cependant pas de moyens suffisants pour aller au-delà de services d'assistance automatisée (autodiagnostic en ligne de cyberincident) et de mise à disposition de ressources en ligne.

Le développement d'actions de sensibilisation sur le terrain, en complémentarité avec l'action de Cybermalveillance, est à soutenir. Des actions de proximité sur l'hygiène numérique, qui intègre le concept de cybersécurité, sont déjà portées par des acteurs locaux dans le cadre d'actions sur l'inclusion numérique.

[3] https://www.cybermalveillance.gouv.fr/

Un partenariat entre Cybermalveillance et le Campus Cyber Grand Est sera mis en place pour mieux coordonner cette complémentarité.

L'information et la sensibilisation à la cybersécurité constituent un des piliers du projet Campus Cyber Grand Est qui sera détaillé dans le chapitre 7.

La sensibilisation des entreprises et des collectivités régionales

La sensibilisation des organisations publiques et privées régionales, dont les systèmes d'information sont plus structurés, est réalisée actuellement par des acteurs de proximité divers : chambres consulaires, agences de développement économiques, associations professionnelles, unités de gendarmerie dédiées à la cybersécurité, offreurs de solutions numériques… Ces actions menées au plan local (départemental au mieux) ne sont ni coordonnées, ni relayées efficacement à un niveau régional.

Cette sensibilisation passe également par des partenaires qui développent des événements reconnus à l'échelle régionale, voire nationale. Outre leur audience directe, ces événements ont un rôle de sensibilisation par les retombées media, qu'ils occasionnent. C'est par exemple le cas de l'association Ad Honores qui met en œuvre le Forum du Rhin Supérieur sur les Cybermenaces depuis 15 ans, dont la notoriété est nationale et dont la Région Grand Est est partenaire.

Dans un souci d'efficience, une coordination des actions de sensibilisation et une mutualisation des ressources est nécessaire à l'échelle de la région. Le projet Campus Cyber Grand Est, détaillé dans le chapitre 7, aura vocation à développer une offre de services en ce sens dans son pilier Information/sensibilisation.

La sensibilisation des jeunes

Par leurs pratiques intensives de la communication et des services en ligne, les jeunes sont particulièrement exposés aux risques cyber, quand bien même les actifs numériques d'un jeune n'ont pas la même valeur unitaire qu'une entreprise ou une collectivité.

Cette exposition est présente des risques plus grands car une part très significative des jeunes mélange, sur leurs terminaux, leurs usages scolaires et leurs usages personnels du numérique et augmente ainsi le risque cyber pour les systèmes éducatifs numériques.

Cette cible de population est également une priorité en matière de sensibilisation car ils sont les futurs actifs de la société et on sait que la cybersécurité n'est réellement efficace qu'avec la mobilisation de tous les acteurs.

La Région Grand Est s'engage à sensibiliser les lycéens à l'hygiène numérique et plus particulièrement à la cybersécurité, dans le cadre du programme Lycée 4.0 et de la fourniture d'un ordinateur portable à chaque élève à son entrée au lycée.

OBJECTIF : La Région Grand Est s'engage à appuyer la coordination des actions de sensibilisation à la cybersécurité du grand public, des collectivités territoriales, des entreprises et des jeunes sur le territoire régional et à favoriser la mutualisation des ressources nécessaires à leur mise en œuvre, à travers le Campus Cyber Grand Est.

2. Préparer l'ensemble des acteurs du Grand Est aux cybermenaces

Consciente que le risque de cyberattaque ne doit pas être un frein à la transformation numérique des acteurs publics et privés régionaux, la Région Grand Est ambitionne d'accompagner ces derniers dans la gestion de ce nouveau risque pour en limiter les occurrences et en prévenir les effets.

Tous les acteurs du territoire régional étant concernés, la Région Grand Est entend initier une dynamique d'accompagnement suffisamment ambitieuse pour que la gestion du risque cyber devienne la norme chez ces acteurs.

Pour permettre à chaque acteur régional d'appréhender une gestion du risque cyber qui lui est spécifique, il est nécessaire d'accompagner celui-ci dans ses projets individuels de développement en matière de cybersécurité.

La sensibilisation à la problématique ayant été abordé précédemment, l'accompagnement passe par une évaluation du niveau de cybermaturité, avant de définir un plan d'actions et de recommandations de cybersécurité. La mise en œuvre de ce plan pourra être accompagné sur le plan financier et par une mise en relation avec des prestataires identifiés.

Pour les entreprises, ce besoin est couvert par les **parcours de transformation** définis dans le volet 2 du Business Act Grand Est et déployés par les services de la Région (voir figure 5).

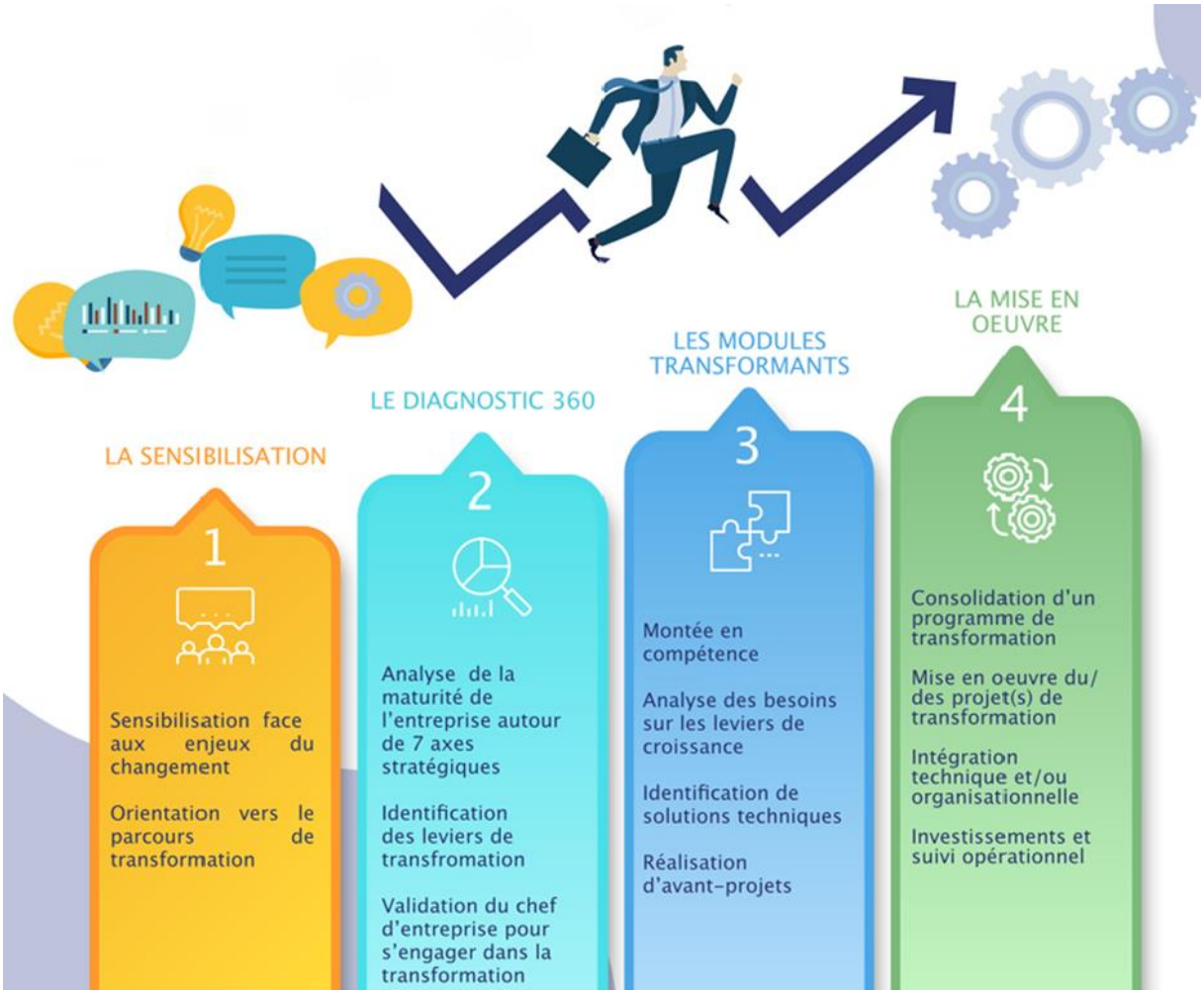

Figure 5 Parcours régional d'accompagnement

La **transformation numérique des entreprises** est une des trois priorités en matière de transformation des entreprises, identifiées dans le Business Act Grand Est. Cela se traduit par l'intégration d'un **axe numérique** parmi les 7 axes stratégiques du **diagnostic 360°** (voir étape 2 de la figure 5) afin d'évaluer le **degré de maturité de l'entreprise** et d'identifier les **leviers de transformation** en matière de numérique.

La **phase d'évaluation et de définition du plan d'action** est couverte par le module transformant en cybersécurité. Celui-ci comprend actuellement le **diagnostic Cybersécurité** adopté par la Commission permanente du 24 juin 2022.

Le Diagnostic Cybersécurité est un outil opérationnel qui permet au dirigeant **d'évaluer le niveau de sécurité du système d'information** de son organisation, tant sur le plan **organisationnel** que **technique**. Il permet d'identifier les **failles éventuelles de sécurité** et conduit à l'élaboration d'une **feuille de route et de remédiation priorisée** adaptée aux besoins de l'organisation.

Il consiste en une mission d'**environ 10 jours/homme confiée à un conseil expert en cybersécurité**, sélectionné préalablement sur appel à candidature par la Région en octobre 2022.

L'intervention est cadrée par la méthodologie et les outils construits par Grand Enov. Le prestataire transmet à la Région (PMO en charge du suivi des parcours) les données d'évaluation et de suivi destinées au pilotage du parcours selon le modèle ci-dessous (voir figure 6).

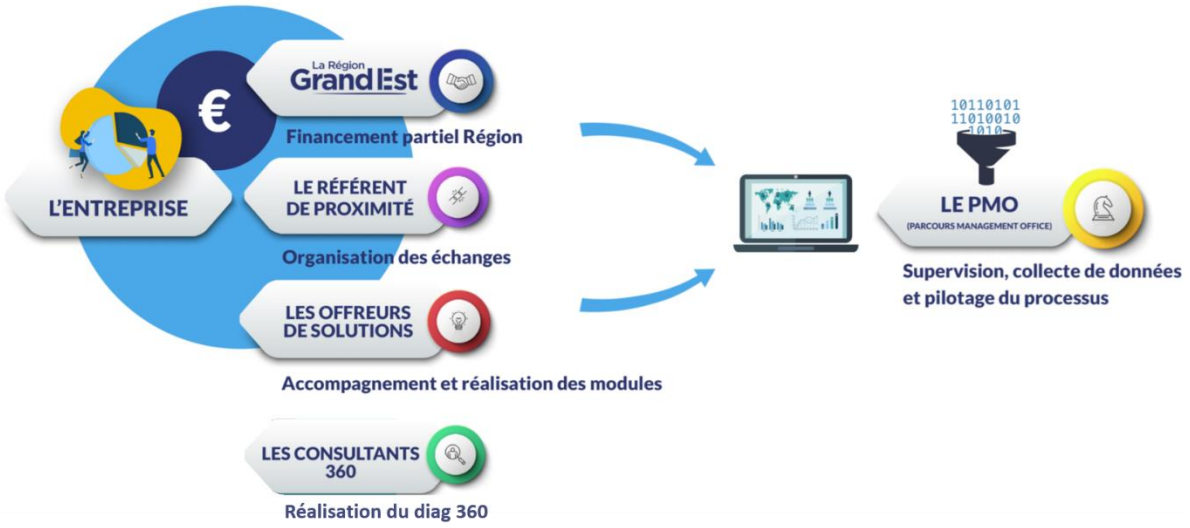

Figure 6 Rôle du Parcours Management Office dans la collecte de données

Grand Enov a élaboré l'outil de diagnostic en se fondant à la fois sur les outils déployés par l'ANSSI[4] (Agence nationale en charge de la cybersécurité) pour le diagnostic des collectivités territoriales (Plan France relance) et sur le socle réglementaire de l'ANSSI. Une phase d'expérimentation conduite pendant l'été 2022 a permis de tester outils et méthodologie.

Cet encadrement strict de la prestation vise à garantir la qualité de celle-ci auprès du bénéficiaire. Elle vise également à assurer à la Région la qualité de la remontée des données structurées anonymisées issues du diagnostic. Elle garantit enfin la meilleure intégration possible du Diagnostic Cybersécurité dans le parcours régional d'accompagnement mis en place par la Région.

L'encadrement permet également de limiter le coût maximum applicable par le prestataire référencé pour réaliser le Diagnostic Cybersécurité à **10 000 € HT**. Le taux de prise en charge financière par la Région est fixé à **50% maximum du coût de la prestation**. Cet encadrement tarifaire vise à rassurer les organisations peu au fait des coûts des prestations en cybersécurité.

Le dispositif de diagnostic Cybersécurité est **ouvert depuis le 20 octobre** à l'ensemble des entreprises régionales.

[4] Agence Nationale de la Sécurité des Systèmes d'Information

Le Business Act Grand Est a posé un objectif de **500 diagnostics réalisés d'ici 2025**.

Les acteurs publics et associatifs régionaux font face à des besoins similaires aux entreprises, sans disposer de dispositif d'accompagnement adapté. La Région Grand Est s'engage donc à **étendre l'éligibilité du dispositif de diagnostic Cybersécurité aux acteurs publics et associatifs régionaux** (collectivités, établissements publics, associations et établissements de santé).

La **phase d'accompagnement à la mise en œuvre de projet** reposera notamment sur la plateforme de mise en relation entre les besoins qualifiés des entreprises issus du parcours d'accompagnement régional et les offres des acteurs de la filière régionale de cybersécurité, référencés à travers le DAS Cybersécurité. Cette plateforme est en cours de développement.

Les aides financières reposent dans un premier temps sur les dispositifs existants, avant d'évaluer dans un second temps si les besoins émergents nécessitent une adaptation des conditions d'éligibilité ou de mise en œuvre de ces aides.

Un projet européen pour la cybersécurité des industriels

Le Grand Est a répondu à l'appel à projet européen relatif à la mise en place d'un EDIH[5] sur le territoire régional, au bénéfice des industries manufacturières. Le projet EDIH Grand Est a été retenu par la commission Européenne le 7 février 2023.

Cet EDIH proposera un accompagnement pour les projets de transformation numérique relatifs à l'Intelligence artificielle, à la cybersécurité et au Calcul Hautes Performances, avec une offre de services innovants tel que le test avant investissement et une mise en réseau d'EDIH partenaires en France et dans les régions transfrontalières.

Ce dispositif dédié aux industriels complètera l'offre d'accompagnement de la Région Grand Est.

OBJECTIF : La Région Grand Est maintient un objectif ambitieux d'accompagner 500 diagnostics régionaux en cybersécurité d'ici 2025 et de favoriser la mise en œuvre des plans d'actions et de remédiation induits au plus tard 12 mois après l'émission du rapport de diagnostic, selon la volonté du dirigeant d'entreprise.

Par son ampleur, cet objectif vise à généraliser la gestion du risque cyber pour tous les acteurs du territoire.

[5] EDIH : European Digital Innovation Hub

3. Améliorer la résilience des organisations face aux cyber attaques, en s'appuyant sur Grand Est Cybersécurité

Les mesures de prévention des cyberattaques ne permettant pas d'éliminer totalement le risque pour les organisations du Grand Est, la Région entend accompagner les victimes pour limiter les effets de ces cyberattaques sur la viabilité des organisations.

En cybersécurité, le risque zéro n'existe pas pour plusieurs raisons :

- La menace cyber en termes de techniques, tactiques, et procédures (TTP) évolue en permanence
- les cyberattaquants se sont professionnalisés et sont très agiles, notamment grâce au Darknet, véritable place de marché de la criminalité. Ils intègrent les dernières technologies numériques au même rythme que les offreurs de solution de cybersécurité (Intelligence artificielle, quantique, …)
- le facteur humain est le maillon faible. La moindre négligence de sécurité d'un utilisateur est une faille potentielle qu'un cyberattaquant peut exploiter pour initier une cyberattaque.

Si l'accroissement du niveau de cybersécurité des organisations, abordé au point 2, contribue à prévenir et réduire le nombre des attaques, il est indispensable de pouvoir accompagner les organisations régionales victimes d'attaques réussies pour en limiter les conséquences néfastes.

« 50% des PME ayant subi une cyberattaque de type rançongiciel disparaissent dans les 6 mois. »

Jean-Noël Barrot, Ministre délégué en charge de la transition numérique, 2022.

Cet accompagnement se fait sous deux formes complémentaires :

- **l'amélioration du niveau de cybersécurité pour préparer l'entreprise** à la gestion d'une attaque et lui permettre de **reprendre son activité au plus vite**.
- Un **dispositif de réponse d'urgence aux victimes d'incidents** cyber, pour assister la victime dans les mesures à prendre une fois l'attaque constatée.

L'amélioration passe par les dispositifs d'accompagnement à l'accroissement du niveau de cybersécurité de l'entreprise, évoqués dans le point 2. Le diagnostic va, par exemple, porter son attention sur la politique de sauvegarde des données de l'entreprise qui est un facteur déterminant de sa cyber-résilience.

La **phase de réaction à une cyberattaque** relève d'une temporalité et de besoins différents. Une capacité de **réponse rapide pour qualifier l'incident et apporter des premières recommandations** a depuis longtemps été modélisé sous la forme de CERT[6] ou de CSIRT[7]. L'ANSSI est chargée notamment de la coordination des CERT/CSIRT français pour coordonner au niveau national le dispositif de réponse à incident et permettre le partage de données d'incidentologie.

[6] Computer Emergency Response Team
[7] Computer Security Incident Response Team

En 2020, l'ANSSI a lancé un appel à candidature auprès des régions françaises pour la création de CSIRT régionaux. L'objectif était d'apporter une réponse aux victimes non couvertes directement par l'ANSSI (Opérateurs de Services Essentiels et Organismes d'Intérêt Vitaux) et non prises en charge via le portail national Cybermalveillance qui adresse les particuliers et les micro-structures sans réel système d'information.

La Région Grand Est s'est portée candidate par un **projet de CSIRT régional adopté en Commission Permanente le 10 septembre 2021**.

Le CSIRT régional Grand Est ou « **Grand Est Cybersécurité** » a vocation à centraliser régionalement **le suivi et la coordination du traitement des incidents** en matière de cybersécurité, depuis la détection jusqu'à la résolution.

C'est un dispositif de permanence téléphonique visant à :

- **Qualifier les incidents** ;
- **Mettre en relation les victimes avec des prestataires de remédiation** préalablement référencés ;
- **Assurer un appui en termes d'informations et de conseils**, notamment pour les poursuites juridictionnelles ;
- Garantir le **partage de données d'incidentologie** avec le réseau des CERT.

Le projet est soutenu dans sa phase d'amorçage par une **subvention de l'ANSSI de 1 million d'euros** pour 3 ans. Il est porté en phase d'incubation par Grand Enov et dispose d'une gouvernance propre associant la Région, les services de l'Etat et des représentants des bénéficiaires et des prestataires référencés.

Le noyau cœur de l'équipe CSIRT a participé entre septembre 2022 et janvier 2023 à un programme obligatoire d'accompagnement de l'ANSSI pour l'ensemble des projets régionaux.

Le référencement des prestataires de réponse à incidents s'appuie sur le travail effectué par le DAS Cyber du GET Numérique.

Le service aux bénéficiaires est disponible depuis le 14 février 2023 via le numéro d'appel **09 70 51 25 25**.

Une fois le service pleinement opérationnel, une réflexion sera lancée sur le modèle économique post-amorçage et le portage définitif du dispositif.

OBJECTIF : La Région Grand Est se donne pour objectif de porter à plus de 75% le niveau de satisfaction des victimes quant à l'accompagnement par le centre de réponse et la prestation de remédiation dès 2024.

4. Soutenir la sortie de crise cyber des organisations

Une attaque cyber d'ampleur touche profondément les victimes, tant dans leurs systèmes d'information que dans les pratiques quotidiennes de leurs collaborateurs. La Région Grand Est entend poursuivre son action au-delà de la crise cyber elle-même pour contribuer à en réduire les effets et à réduire plus globalement la menace.

Grand Est cybersécurité, le CSIRT régional Grand Est, a pour mission d'assurer un **suivi des victimes** mises en relation avec des prestataires dédiés à la remédiation. Ce suivi permet notamment d'accompagner les victimes sur les 2 phases de la remédiation :

- La **mise en sécurité du système d'information**, qui est au cœur de la gestion de crise abordée au point 4.
- La **reconstruction du système d'information**, dont l'ampleur dépendra du niveau de dégâts constaté et des mesures de prévention mises en œuvre au préalable. Le suivi peut alors permettre des mises en relation avec d'autres offreurs de solutions identifiés par le GET Numérique et une orientation vers les dispositifs d'aide financière définis dans le cadre du parcours régional d'accompagnement.

La **lutte contre la cybercriminalité nécessite une judiciarisation des cyberattaques** pour permettre la mobilisation des forces de l'ordre et de la justice pour faire tomber les réseaux criminels, souvent dans le cadre de coopérations internationales.

La victime de cyberattaque reste seule décisionnaire de sa volonté de déposer plainte. Le CSIRT régional Grand Est cybersécurité a pour mission de l'accompagner dans la démarche le cas échéant.

Une **convention de partenariat avec la Gendarmerie Nationale**, portant sur les **relations à établir pour accompagner le dépôt de plainte**, est soumise au vote de la Commission permanente de la Région du 24 mars 2023. Une convention similaire sera proposée avec la **Police Nationale** prochainement.

En matière de cybersécurité, le **partage de données entre opérateurs** sur les failles dans les outils, sur les cyberattaques et plus largement sur l'état de la menace est un facteur clé de réduction de cette menace.

Cette approche collective est au cœur du réseau des CERT dont Grand Est Cybersécurité va faire partie avec l'ensemble des CSIRT régionaux.

Le **développement au niveau régional du partage d'informations sur la menace cyber** est également l'une des missions que doit porter le **Campus Cyber Grand Est** qui sera détaillé au point 7.

OBJECTIF : La Région Grand Est se donne pour objectif de réduire la gravité des impacts des cyberattaques observées dans le Grand Est d'ici 2025.

5. Favoriser le développement de la filière régionale de Cybersécurité

La Région Grand Est ambitionne d'accompagner la structuration de la filière régionale de cybersécurité, pour disposer sur le territoire du Grand Est d'une réponse à la demande de cybersécurité des acteurs publics et privés régionaux.

La filière numérique en Grand Est représente 4,25% des emplois dans le numérique en France contre 7,47% pour l'ensemble des emplois. Elle est constituée essentiellement de TPE et PME, avec quelques ETI[8] d'envergure nationale, voire européenne.

Sa structuration s'est faite au fil des années autour d'acteurs infra-régionaux de type associations professionnelles ou clusters, à l'exception notable de Numeum[9]. Les offres de services n'étaient pas uniformes et les périmètres de sous-domaines du numérique couverts étaient variables.

En matière de cybersécurité, le panorama régional est similaire avec 2 ETI et une centaine d'offreurs de solutions identifiés. La structuration s'est faite partiellement sur le plan régional autour des CLUSIR Est et Champagne Ardennes, qui fédèrent offreurs de solutions et utilisateurs, d'autres offreurs se tournant vers des associations professionnelles nationales (ACN, Hexatrust, …).

Le volet 2 du Business Act Grand Est a acté la nécessité d'améliorer la structuration de la filière numérique à l'échelle régionale par la création du Grand Est Transformation (GET) Numérique.

Parmi les communautés thématiques identifiées comme stratégiques pour la Région, la cybersécurité a fait l'objet d'une action prioritaire et le DAS Cybersécurité a été lancé le 5 juillet 2022.

Le DAS Cybersécurité agit comme un think tank régional, un laboratoire d'idées qui réunit et fédère des experts du domaine afin de s'assurer que les offreurs du GET soient toujours alignés avec la réalité de la technologie et des usages actuels, mais également maintenus au meilleur état de l'art.

Ses missions sont les suivantes :

- Elaboration courant 2023, mise en œuvre et suivi d'une **feuille de route à 360°** (technologies, usages, compétences, chaines de valeur, …)
- Contribution au **déploiement des projets structurants** du volet 2 du Business Act Grand Est :

[8] Entreprises de taille intermédiaire, entre 250 et 2 000 salariés
[9] syndicat professionnel national disposant d'une branche régionale en Grand est

  - aide à l'élaboration des outils du parcours régional d'accompagnement des entreprises,
  - référencement des offreurs de solutions de cybersécurité, y compris les offreurs de solutions d'accompagnement impliqués dans les phases d'audit et de mise en œuvre,
  - contribution à l'analyse des besoins en compétences de cybersécurité dans les entreprises régionales
- **Vision prospective et clés de lecture** pour comprendre les évolutions technologiques et d'usages, à destination des décideurs régionaux

Co-animé par Grand Enov et par un offreur régional de solutions de cybersécurité, le DAS Cybersécurité est organisé en 2 niveaux :

- La **communauté des offreurs au sens large** du terme, sous réserve d'expertise, qui se réunit 1 fois par an ;
- Le **groupe de travail cœur** composé de 10 à 20 membres se réunissant en fonction de l'actualité de la cybersécurité, au minimum de manière trimestrielle.

OBJECTIF : La Région Grand Est a confié l'animation de la communauté des acteurs de la cybersécurité à l'agence régionale Grand Enov+ avec l'objectif

- **de densifier l'offre régionale en permettant aux offreurs régionaux de capter, à terme, 70% des projets de cybersécurité issus du parcours régional de transformation**
- **de disposer une offre régionale au meilleur niveau de l'état de l'art en favorisant la connexion des offreurs aux acteurs académiques et en supportant leur projet d'innovation**
- **de disposer d'une feuille de route cyber courant 2023, fruit du travail collectif des offreurs**
- **de rendre nos offreurs plus robustes en accompagnant leur montée en compétences**
- **d'augmenter le niveau d'excellence global de l'offre régionale par la mise en place d'une dynamique chez les offreurs pouvant leur donner accès à horizon 3 ans aux labellisations sectorielles nationales et internationales**

6. Développer les compétences en cybersécurité

La Région Grand Est se donne pour ambition de réduire le déficit de compétences en cybersécurité dans le Grand Est alors que la demande va croître de la part des entreprises utilisatrices et de celle des acteurs de la filière.

L'accroissement de l'offre de compétences en cybersécurité passera par une plus grande attractivité des métiers de la cybersécurité et une offre de formation plus adaptée aux besoins, tant sur le plan quantitatif que qualitatif.

La mise en œuvre des 3 axes présentés précédemment est conditionnée par la disponibilité d'un vivier suffisant de compétences métier en cybersécurité.

A l'instar des compétences dans les métiers du numérique, la France souffre d'un **déficit de compétences en cybersécurité à hauteur de 15 000 postes** (source ANSSI 2021)[10].

Environ **300 postes en cybersécurité sont à honorer en Grand Est[11].** Sans action spécifique, la mise en œuvre de la feuille de route régionale ne fera qu'accroître ce déficit.

Ce déficit a de multiples origines :

- La transformation numérique de la société et de l'économie croît à un rythme plus rapide que la capacité des systèmes éducatif et de formation à recruter et à répondre à la demande croissante induite.
- Les **métiers du numérique** en général pâtissent encore d'une **mauvaise image** ou d'un a **priori d'inaccessibilité auprès de certaines populations** jeunes ou en reconversion, notamment la population féminine.
- Au sein des métiers du numérique, **la cybersécurité pâtit d'une image encore plus mauvaise**, souvent appuyé par des médias en recherche de sensationnalisme[12].
- La diversité des métiers de la cybersécurité (50 métiers identifiés par le Campus Cyber) reste méconnue, l'attention restant concentrée sur les profils techniques d'ingénieur.
- Le tissu d'employeurs en cybersécurité en Grand Est est constitué essentiellement de PME, qui ne disposent pas des moyens de faire évoluer ces a priori en termes d'image.
- Les formations dédiées à la cybersécurité en Grand Est ciblent plutôt des profils scientifiques niveau ingénieurs ou Master 2. Un déficit de profils de techniciens de la cybersécurité est anticipé au niveau régional comme au niveau national.
- Les femmes sont très peu représentées (30%) dans les métiers du numérique et de la cybersécurité
- Le caractère transfrontalier de notre région expose notre filière à une concurrence des marchés francilien, luxembourgeois, allemand et suisse pour l'attractivité des talents.

La problématique d'image entraîne une difficulté pour certains organismes de formation à remplir leur formation en cybersécurité, ce qui limite le développement de nouvelles formations.

Au-delà de la sensibilisation aux enjeux du numérique, des actions spécifiques sont à mener auprès du grand public pour **sensibiliser aux métiers de la cybersécurité**, qui sont en tension, bien rémunérés et porteurs de sens. 3 populations sont particulièrement visées :

- **les jeunes** et leurs parents,
- **les populations féminines**, faiblement présentes sur les métiers du numérique et encore moins présentes sur les métiers de la cybersécurité

[10] "les profils de la cybersécurité 2021 enquête de l'ANSSI" 15665 postes à pourvoir en France,
[11] Projection considérant le poids de la filière cyber régionale Grand Est dans la filière nationale : 2% en Grand Est, soit 300 postes
[12] Habillage de l'émission C dans l'air : spéciale : « Cyber : la guerre est déclarée », France 5 - dimanche 9 octobre 2022

- **les personnes en reconversion professionnelle**

Une action sera menée pour développer la communication et la mise en visibilité de l'offre de formation initiale et continue régionale sur la cybersécurité.

Par ailleurs, les **travaux menés dans le cadre du GET numérique sur l'anticipation des besoins en compétences** vont amener à rapprocher l'expression fine des besoins des acteurs de la filière cybersécurité avec l'offre des organismes de formation.

La Région pilote actuellement une gestion prévisionnelle des emplois et compétences territoriale dans le cadre d'une action prioritaire identifiée dans le cadre de la démarche du Business Act. Dans ce cadre, une enquête régionale **sur les besoins en compétences numériques des entreprises est en cours et les résultats sont prévus d'ici fin 2023**. Parallèlement, la Région a lancé un état des lieux des formations initiales et continues sur le numérique et l'industrie 5.0.

La Région croisera les besoins exprimés et l'état des lieux des formations pour préconiser l'adaptation, le développement ou la création de formations initiales ou continues.

La Région, dans le cadre de son programme régional de formation pour les demandeurs d'emploi, adapte son offre pour répondre à la demande des entreprises régionales et a déjà intégré la cybersécurité dans les métiers couverts.

Deux **Campus des Métiers et des Qualifications** (CMQ) du Grand Est sont dédiés au numérique (CaMéX-IA en Moselle et CMQ Industrie du futur et numérique dans le Haut-Rhin) et sont déjà cofinancés par la Région. Un soutien de la Région à l'intégration plus forte de la thématique cybersécurité dans les CMQ existants ou une réflexion à la création d'un CMQ dédié ou équivalent pourra être proposé.

La Région a également missionné Numeric'Emploi Grand Est pour **référencer et mettre en visibilité** sur son portail web, d'ici fin 2023, **l'ensemble de l'offre de formation initiale et continue sur le numérique au niveau régional** ; à ce titre plus de 80 opérateurs de formation publics et privés sont mobilisés. Des cartographies de l'offre de formation seront également proposées sur les différentes familles de métiers du numérique dont la cybersécurité

Ces outils contribueront à une meilleure visibilité de l'offre de formation auprès des publics et des entreprises.

OBJECTIF : La Région Grand Est se donne pour objectif en 2023 d'affiner l'analyse des besoins en compétences en cybersécurité auprès des entreprises utilisatrices et auprès de la filière régionale et d'améliorer la visibilité de l'offre régionale de formation initiale et continue sur les métiers de la cybersécurité.

7. Une mise en œuvre de la feuille de route fédérée autour d'un Campus Cyber Grand Est

Pour réaliser son ambition d'un territoire régional de confiance où le risque cyber est maîtrisé, la Région Grand Est entend fédérer toutes les acteurs régionaux de la cybersécurité, y compris les utilisateurs, pour « jouer collectif » face à une menace commune.

Les axes du plan régional de cybersécurité ont vocation à concerner l'ensemble des organisations régionales comme bénéficiaires et l'ensemble de l'écosystème régional de cybersécurité comme parties prenantes.

Confronté à une situation similaire au niveau national, le Président de la République a initié en 2019 une dynamique fédérative auprès de l'écosystème national de cybersécurité : réunir dans un **lieu totem** les acteurs de la sécurité numérique pour **mieux protéger la société** et **faire rayonner l'excellence française du domaine**.

Cette **initiative publique - privée**, Le **Campus Cyber**, immeuble de 26 000 m^2 à Paris-La Défense a ouvert en février 2022 et accueille 250 acteurs dont 115 résidents représentant l'ensemble de l'écosystème : offreurs de solutions, utilisateurs, acteurs étatiques, organismes de formation, startups, laboratoires.

Le Campus Cyber ancre son action sur 4 piliers complémentaires :

- **Opérations** : partager les données pour renforcer la capacité de chacun à maîtriser le risque numérique ;
- **Sensibilisation/Formation** : aider à la formation initiale et continue des différents publics (agents de l'État, salarié(e)s, étudiante(s), personnels en reconversion…) pour une montée en compétence globale de l'écosystème ;
- **Innovation** : développer des synergies entre les acteurs publics et privés pour orienter l'innovation technologique en matière de cybersécurité et renforcer son intégration dans le tissu économique, notamment au travers des startups ;
- **Mobilisation** : proposer un lieu vivant et ouvert dédié à la programmation d'événements innovants propice, aux échanges et à la découverte des évolutions de la société numérique de confiance.

Le constat a rapidement été partagé de la **nécessité de disposer de relais sur le terrain** pour décliner cette dynamique dans l'ensemble du tissu économique et administratif. Les services de la Région Grand Est et d'autres régions ont été associés en 2021 à la définition d'une **Charte des Campus Cyber territoriaux**, préalable à un **appel à candidature lancé par la SAS Campus Cyber en 2022** auprès des régions françaises pour proposer un projet de Campus Cyber territorial.

Les contraintes de la Charte visent essentiellement :

- La nécessité d'**agir sur les 4 piliers** du Campus Cyber ;
- Une **gouvernance très ouverte** à l'ensemble de l'écosystème cyber régional, de type collèges catégoriels ;
- Un **soutien fort** du projet par la Région.

Pour saisir cette opportunité de mobiliser l'ensemble des acteurs régionaux de la cybersécurité autour d'un projet fédérateur, le Président de la Région a souhaité pendant l'été 2022 la création d'un **groupe de travail de préfiguration** rassemblant services de la Région, l'agence Grand Enov+, représentants d'utilisateurs, d'offreurs de solutions et d'académiques.

Le Groupe de travail élabore :

- une offre de services,
- un modèle économique,
- des modalités de fonctionnement et de gouvernance
- des statuts d'une structure porteuse

La **conclusion des travaux** est attendue pour le premier trimestre 2023 avant d'être partagé avec l'écosystème régional de cybersécurité. Le dossier de candidature sera soumis au vote des élus de la Région au deuxième trimestre 2023, puis transmis à la SAS Campus Cyber pour validation. L'objectif est de **lancer l'initiative régionale sur le second semestre 2023**.

Au vu de la géographie et de l'organisation régionale du Grand Est, un **équilibre** est à définir **entre proximité de terrain et masse critique de l'écosystème cyber territorial** pour assurer la pérennité de la dynamique. Cet équilibre peut varier selon les services proposés : les actions de sensibilisation et d'information nécessitent une proximité de terrain quand le soutien à l'innovation atteint une masse critique uniquement au niveau régional.

De cet équilibre dépendra la structuration du Campus Cyber Grand Est entre niveau régional et niveau territorial et l'incarnation physique qui en découlera.

Une spécialisation sur une **cybersécurité transfrontalière** pour le Campus Cyber Grand Est apparaît déjà comme une évidence au vu de la situation géographique et des besoins concrets des acteurs régionaux.

Cette spécialisation se traduit par des **objectifs de convergence réglementaire** là où la région peut intervenir et des **projets opérationnels transfrontaliers** sur le partage de données, sur les modalités de gestion de crise cyber, sur l'accès aux compétences cyber, sur l'innovation en cybersécurité…

OBJECTIF : La Région Grand Est a pour objectif de lancer au second semestre 2023 un Campus Cyber Grand Est ouvert à tous les acteurs de la cybersécurité en Grand Est et travaillant en réseau pour apporter la cybersécurité au plus près des utilisateurs.

Le Campus Cyber Grand Est vise à coordonner et mutualiser les efforts et ressources de la communauté régionale en matière de sensibilisation, de développement des compétences, de partages de données, d'innovations et de coopérations transfrontalières.

Conclusion

Ce plan régional thématique répond à une approche spécifique à la cybersécurité, qui privilégie la fédération des acteurs de l'écosystème régional pour protéger des milliers d'acteurs publics et privés face à une menace mondialisée aux effets délétères et pour accroître la part de marché de notre filière régionale sur un marché en très forte croissance.

En matière de protection des acteurs régionaux, le plan reste encore à connecter avec d'autres initiatives en développement, visant à faire du Grand Est un territoire de confiance :

- Le **Cloud souverain régional**, action phare du volet 2 du Business Act Grand Est, dont les études de faisabilité sont en cours ;
- Les démarches visant à assurer le **continuum de sécurité** en Grand Est par une mobilisation des acteurs territoriaux autour des défis organisationnels et opérationnels posés par la sécurité dans son ensemble. Cela passe notamment par un décloisonnement des pratiques des acteurs publics et des acteurs privés en la matière, en particulier face à la menace cyber.

Pour le développement de la filière régionale, le plan s'intègre dans la stratégie de développement des offreurs de solutions, déjà structurée par le Business Act Grand Est en 2020 et 2021, aux côtés du plan régional Intelligence Artificielle.

En conclusion, voici les facteurs-clés de succès de ce plan régional de Cybersécurité :

- Densifier les acteurs de la cybersécurité et les fédérer sur le long terme au sein d'un Campus Cyber Grand Est,
- Adapter dans la durée les ressources mises en œuvre par la Région, selon les besoins des acteurs régionaux,
- Savoir accompagner toute demande en cybersécurité (du plus simple au plus complexe),
- Assurer la disponibilité de compétences en cybersécurité sur l'ensemble du territoire régional,
- Développer un cadre de coopération avec les partenaires transfrontaliers pour garantir un espace de confiance à l'échelle de ces territoires cumulés.