La Région
Auvergne-Rhône-Alpes

Feuille de route cybersécurité

Introduction

1. Contexte et enjeux

En l'espace de quelques années, le **numérique est devenu un moteur essentiel de transformation économique, sociale et culturelle** des organisations humaines et des sociétés. A la fois langage commun et outil universel, il constitue aussi un **fort moteur de croissance**. A ce titre, il est pour l'économie de la région Auvergne-Rhône-Alpes un levier stratégique. Cependant, la capacité du numérique à structurer et accompagner l'ambition d'une économie régionale toujours plus dynamique et innovante dépend de multiples facteurs. Notamment, elle induit de répondre aux enjeux et défis de la sécurité des réseaux de télécommunication et des systèmes informatiques ainsi que de la protection des données qu'elles soient **d'intérêt général, qu'elles soient constitutives des actifs de nos entreprises ou qu'il s'agisse de données personnelles**.

L'augmentation de l'activité en ligne, le caractère central des systèmes d'information, le recours massif aux clouds, les objets connectés… augmentent de fait la « surface d'attaque » et créent de nouvelles vulnérabilités. En parallèle, les **usages délictueux et malveillants des technologies** croissent. Les innovations (Intelligence Artificielle par exemple) offrent sans cesse de nouvelles opportunités aux attaquants et exigent une mise à niveau permanente.

Enfin, le **contexte géopolitique** (Russie-Ukraine, Chine, Moyen-Orient, nouvelle doctrine américaine…) induit un développement de la conflictualité en ligne avec des attaques sur des opérateurs sensibles et des opérations de déstabilisation.

Cette augmentation des risques et ce besoin en cybersécurité est de plus en plus prégnant et apparait donc comme le **revers de la digitalisation.**

De fait, la **cybermenace** et les faits de cyber-malveillance se sont nettement **intensifiés** au cours des mois passés.

- Près de 47% des entreprises françaises interrogées par le CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) ont constaté au moins une cyberattaque significative en 2024
- Selon le dernier rapport sur la sécurité des applications (2024) de l'entreprise américaine Cloudflare (offreur de solutions « cloud » sécurisées) qui a réalisé une étude auprès de 432 dirigeants et décideurs informatiques d'entreprises françaises, 31 % des personnes interrogées ont subi au moins une attaque au cours des 12 derniers mois.
- Ce même rapport indique une nette augmentation du trafic internet malveillant qui atteindrait désormais 7% du trafic global.
- Le nombre total d'attaques par rançongiciel portées à la connaissance de l'ANSSI (’Agence Nationale de la Sécurité des Systèmes d'Information) ont augmenté de près de 30% par rapport à 2022

Les impacts d'une cyberattaque peuvent être nombreux pour l'entreprise victime : perturbations ou arrêt de la production, indisponibilité de site web, perte d'image, impact médiatique, compromission d'informations, fuites de savoir-faire, perte financière directe liée aux transactions frauduleuses, perte de chiffre d'affaires, retards de livraison, sanctions par les autorités (CNIL)... Toujours selon le dernier rapport de Cloudflare :

- 72 % des entreprises attaquées ces 12 derniers mois évaluent le sinistre à 940 000 euros au moins, tandis que les 28 % restant chiffrent les conséquences à près de 1,9 million d'euros.
- Un tiers des sondés déclarent que leur organisation a dû mettre ses projets de développement sur pause à la suite d'une attaque.
- 22 % des organisations ont licencié des collaborateurs à cause des répercussions financières des cyberattaques.

Selon l'ANSSI, il n'y a pas de spécificité régionale dans la nature des cybermenaces : actuellement, les attaques sont majoritairement non-ciblées (démarche systématique de recherche de faille), ont une motivation criminelle et utilisent les rançongiciels (programme malveillant chiffrant les données dans un but d'extorsion).

Pour répondre à cette menace pesant sur ses acteurs économiques, la région Auvergne-Rhône-Alpes dispose de nombreux atouts.

D'abord **sa filière numérique et cybersécurité est dynamique** : le recensement réalisé par l'agence Auvergne-Rhône-Alpes entreprises en 2024 a identifié 387 établissements relevant de la filière cybersécurité. 15% sont des grands groupes, 44% des PME, 36% des TPE ou des starts-ups.

Ensuite son **écosystème de formation** comptant des grandes écoles d'ingénieurs généralistes, des écoles informatiques, des écoles spécialistes de la cybersécurité et des universités propose une offre de formations en cybersécurité large. Renforcé par le plan Région des Ingénieurs et des Techniciens, cet ensemble comptabilise à date plus de 50 formations initiales en cybersécurité en Auvergne-Rhône-Alpes. 5 écoles établies au Campus Région du numérique (les Mines, CSB, IT Akademy, IEQT et M2I) proposent d'ailleurs des cursus de ce type.

Auvergne-Rhône-Alpes constitue en outre un **pôle de recherche majeur en cybersécurité** avec pas moins de 8 centres académiques d'excellence. La Région constitue ainsi le second pôle national de recherche accueillant 238 chercheurs soit près de 165 équivalents temps plein consacrés à la thématique. Ses domaines d'excellence sont la sécurité du matériel (CEA-Leti, laboratoire Hubert Curien, LCIS, TIMA) et la cryptographie post-quantique (LIP Lyon et l'ERC Prometheus).

Enfin, la Région peut s'appuyer sur les **acteurs de l'écosystème numérique**, associations, pôles et clusters, œuvrant auprès des entreprises et/ou de la filière : Digital League (cluster des entreprises du numérique), ENE Auvergne Rhône-Alpes (association d'accompagnement à la digitalisation des entreprises), ADIRA (Association régionale des professionnels des systèmes d'information), CLUSIR (Club de la Sécurité des Systèmes d'Information), Minalogic (pôle de compétitivité des technologies du numérique). Ces structures collaborent déjà entre elles, notamment dans le cadre des Journées de la Cyber, coorganisées par les 5 acteurs susnommés auxquels on peut ajouter le Cluster EDEN, le Cybercercle et tous les résidents du Campus Région du numérique.

2. Cadrage institutionnel

La stratégie européenne de cybersécurité

La cybersécurité a été affichée comme une priorité politique et économique pour l'Union européenne, justifiée par le contexte international. Sa stratégie de cybersécurité vise à garantir un environnement numérique sécurisé pour les utilisateurs, à renforcer la résilience face aux cybermenaces, à garantir la sécurité des citoyens et des entreprises.

Présentée en décembre 2020, cette stratégie repose sur trois axes principaux : la résilience, la souveraineté technologique et la capacité opérationnelle à prévenir, dissuader, détecter, et répondre aux cyberattaques.

Plusieurs directives européennes cadrent le contexte réglementaire, fixent des normes minimales et guident ainsi la mise à niveau des entreprises et de toutes les autres entités concernées :

- **Cybersecurity Act** (juin 2019) : définit un cadre européen de certification de cybersécurité pour les fabricants et fournisseurs de produits, services et processus des technologies de l'information et de la communication (TIC) leur donnant un ensemble d'exigences de sécurité.
- **NIS2 -Network and Information Security** (décembre 2022) définit des mesures de gestion des risques en matière de cybersécurité minimales à mettre en œuvre par un certain nombre d'entités (incluant des administrations de toutes tailles et des entreprises allant des PME aux grands groupes). 18 secteurs et environ 600 types d'entités différentes seront désormais régulées. Sa transposition en droit français est en cours.
- **DORA** (décembre 2022) : dédié à la résilience opérationnelle numérique des entités financières (secteur bancaire et financier, assurance, gestion d'actifs, marchés…) qui doivent s'assurer qu'elles peuvent « résister, répondre et se rétablir » face à toute perturbation opérationnelle grave liée aux technologies de l'information et de la communication. Il concerne aussi tous leurs fournisseurs de services TIC.
- **IA Act** (août 2024) : centré sur les Systèmes d'intelligence artificielle, il prévoit pour eux une série d'obligations de sécurité (gestion des risques, gouvernance des données, surveillance humaine…)
- **Cyber Resilience Act** (octobre 2024) : aucun produit comportant des éléments numériques (logiciels et objets connectés) ne peut être mis sur le marché s'ils ne satisfait pas à des exigences essentielles de cybersécurité

La stratégie nationale pour la cybersécurité

Lancée le 18 février 2021, elle vise à renforcer la sécurité des systèmes d'information en France face aux menaces croissantes. Elle repose sur cinq priorités :

- Développer des solutions souveraines et innovantes de cybersécurité ;
- Renforcer les liens et synergies entre les acteurs de la filière ;
- Soutenir la demande (individus, entreprises, collectivités et Etat), notamment en sensibilisant mieux, tout en faisant la promotion des offres nationales ;
- Former plus de jeunes et professionnels aux métiers de la cybersécurité, fortement en déséquilibre ;
- Soutenir le développement des entreprises de la filière via un abondement en fonds propres.

Cette stratégie vise à créer un environnement numérique sûr et résilient, capable de protéger les intérêts nationaux et de soutenir la croissance économique. Elle met l'accent sur la coopération entre les différents acteurs et sur l'importance de l'innovation pour faire face aux défis futurs.

Les principaux opérateurs spécialisés au niveau national sont :

- L'**ANSSI** est l'agence gouvernementale chargée de la protection des systèmes d'information de l'Etat, des opérateurs d'importance vitale et des entreprises stratégiques. Elle assure la veille, la prévention, la détection et la réponse aux cyberattaques ainsi que la promotion des bonnes pratiques de cybersécurité
- **Cybermalveillance.gouv.fr** est une plateforme portée par un Groupement d'Intérêt Public « Action contre la Cybermalveillance ». Elle fournit des informations de prévention et une assistance aux particuliers, entreprises, collectivités locales et associations confrontés à un acte de cybermalveillance.
- Le **Campus Cyber** situé à La Défense vise à fédérer la communauté de la cybersécurité et à développer des synergies entre ses différents acteurs : entreprises, services de l'Etat, organismes de formation, acteurs de la recherche, associations…

Une nouvelle brique à la stratégie régionale

Depuis 2017 et l'adoption de sa **feuille de route numérique** régionale, la Région a élevé au rang de **priorité la digitalisation des entreprises** et leur accompagnement dans cette transition. La **création du Campus Région du numérique** à Charbonnières-les-Bains l'a doté d'un outil opérationnel et puissant pour fédérer l'écosystème et impulser le développement des compétences nécessaires.

Sa stratégie régionale pour le soutien à la recherche, au développement et à la diffusion des outils **d'intelligence artificielle partagée avec l'Etat** a complété cet engagement en faveur de l'innovation et de l'adoption des nouveaux outils numériques.

Une stratégie dédiée au numérique de confiance et à la cybersécurité vient donc compléter naturellement cette politique régionale. D'ailleurs, les 5 **orientations stratégiques du Plan Auvergne-Rhône-Alpes 2022 – 2028 pour l'économie, l'emploi, la formation et l'innovation**, ont un écho à cette préoccupation en matière de cybersécurité :

- **Soutenir les relocalisations en misant sur l'industrie :** sécuriser les acteurs industriels et faire d'Auvergne-Rhône-Alpes la première région adressant prioritairement le thème de cybersécurité industrielle est une déclinaison logique de cet axe.
- **Répondre aux deux grands défis de demain : la digitalisation et la décarbonation des entreprises :** les outils et démarches de digitalisation doivent être sécurisés pour être efficients.
- **Orienter et former vers les métiers qui recrutent et les filières d'avenir :** la cybersécurité relève clairement de ces métiers d'avenir.
- **Faire d'Auvergne-Rhône-Alpes la région des ingénieurs, des techniciens et des scientifiques :** les domaines mathématiques, informatiques et cryptographiques sont, de fait, au cœur des solutions de cybersécurité.
- **Miser sur les forces de la région : la recherche et l'enseignement supérieur ainsi que les 13 filières d'excellence identifiées par la Région :** le numérique constitue l'une de ces filières tandis que les autres, à commencer par la santé et l'énergie, sont sensibles à la cybersécurité de leurs installations et applications, ainsi qu'à la protection de leurs données.

La cybersécurité apparaît donc comme un enjeu transversal et fait, en outre, écho à l'ambition régionale de contribuer à l'amélioration de la sécurité, préoccupation majeure de l'ensemble des Auvergnats et Rhônalpins. Sa **politique globale de sécurité**, dans l'ensemble des domaines de sa compétence et ceux pour lesquels le code général des collectivités territoriales lui permet d'intervenir, établie par le **Plan régional de sécurité adopté le 19 juillet 2021**, prévoit d'agir au bénéfice des entreprises sur la thématique de la cybersécurité en élaborant un plan régional en matière de sécurité numérique.

Enfin, il convient de rappeler la **perspective de l'organisation des Jeux Olympiques et paralympiques 2030 dans les Alpes Françaises** qui induit de préparer les acteurs du territoire. A titre de premier retour d'expérience, l'ANSSI a annoncé avoir eu connaissance de 548 événements de cybersécurité affectant des entités en lien avec l'organisation des Jeux Olympiques et Paralympiques de Paris 2024 entre le 8 mai et le 8 septembre 2024 : indisponibilités (attaques par DDoS), compromissions ou tentatives de compromission, divulgations de données, signalements de vulnérabilités... Parmi ces évènements, 83 incidents constituent des événements de sécurité pour lesquels un acteur malveillant a conduit des « actions avec succès sur le système d'information de la victime ».

3. Concertation pour l'élaboration de la présente Feuille de Route

Depuis le début de l'année 2024, le Campus Région du numérique a mené un travail de coordination et de mutualisation pour emmener dans une réflexion commune **7 acteurs régionaux du numérique** : Digital League, ENE Auvergne-Rhône-Alpes, ADIRA, CLUSIR, Minalogic, SWARM, Auvergne-Rhône-Alpes Entreprises.

Ce collectif partage la préoccupation de l'accroissement des cybermenaces pesant sur les acteurs économiques régionaux, en particulier dans l'industrie et vers les PME, et le constat d'un manque de culture du risque cyber, de préparation et de résilience des entreprises.

Afin de faire émerger une contribution commune, une équipe de consultants a appuyé ce travail collectif d'analyse, de benchmark et de priorisation. Il a abouti à une liste de propositions d'action incluant notamment l'émergence d'un « Campus Cyber » régional. Ces propositions ont servi de socle à l'élaboration de la présente feuille de route régionale cybersécurité.

4. Objectifs et principes de la feuille de route cybersécurité Auvergne-Rhône-Alpes

Ce présent document **constitue le Plan régional de cybersécurité et de sécurité numérique, soit l'une des mesures (I.4.b) du Plan régional de sécurité adopté en AP du 19 juillet 2021** prévues au titre de la compétence Développement économique.

Il s'agit d'identifier et mettre en œuvre des actions de renforcement en matière de cybersécurité, tenant compte des multiples enjeux budgétaires, humains, économiques, organisationnels et de se doter d'un outil de structuration et de coordination.

La Région Auvergne-Rhône-Alpes souhaite mobiliser dans un élan collectif l'ensemble du monde économique, des acteurs académiques et des spécialistes du numérique pour **faire de la région un territoire reconnu de sécurité numérique, innovant et réactif face aux menaces**. En outre, Auvergne-Rhône-Alpes souhaite **devenir la Région européenne de référence en matière de cybersécurité industrielle**.

Les **objectifs stratégiques de la Région** qui structurent la présente Feuille de route cybersécurité sont :

- **Protéger les entreprises** de la Région et renforcer leur appréhension des risques cyber afin de mieux y faire face : par un soutien à des actions de sensibilisation et d'accompagnement des entreprises.
- **Animer et développer la filière cybersécurité** régionale, en mettant notamment en visibilité les offreurs de solution régionaux et en favorisant la recherche et l'innovation.
- **Développer les compétences** disponibles sur le territoire en matière de cybersécurité : en valorisant les métiers et en soutenant les structures de formation.
- Mettre en place une **gouvernance régionale** adaptée de la thématique et faire du **Campus Région du numérique un lieu totem** de la cyber.

Ses principes d'action peuvent être synthétisés comme suit :

- **Travailler collectivement** : la région Auvergne-Rhône-Alpes compte de nombreux réseaux, engagés au service d'une meilleure sécurité numérique des acteurs économiques régionaux. Il s'agit pour la Région d'intervenir en animateur et chef de file et d'assurer un lien avec les réseaux nationaux et européens
- **Ne pas se substituer aux compétences régaliennes** ni pallier d'éventuelles insuffisances de moyens ou d'organisation de la part de l'Etat : la Région n'a par exemple pas vocation à porter la création d'un centre de résolution des incidents de cybersécurité placé sous la tutelle de l'ANSSI.
- **Donner la priorité à la prévention :** toute politique de sécurité vise à empêcher la survenance de l'incident. Des services existent pour accompagner et conseiller les entreprises victimes. La Région ne souhaite pas créer de doublons et porter des dispositifs spécifiques sur les volets « réponses à incident » et « remédiation ».
- **S'appuyer sur le Campus Région du numérique** : ouvert en janvier 2021, accueillant déjà des formations dédiées à la cybersécurité, des consortiums industriels travaillant sur ce thème et des entreprises du domaine, il constitue naturellement un « camp de base » pour développer la sécurité numérique en Auvergne-Rhône-Alpes.

Dans une logique pragmatique, cette feuille de route pourra être complétée en fonction des besoins sous forme de délibérations à caractère opérationnel, notamment lorsque des dispositifs apparaîtront nécessaires pour répondre à de nouveaux besoins.

Plan d'action

Les actions menées par la Région, dans le cadre de ses compétences, en faveur d'une cybersécurité renforcée au bénéfice de son économie se déploient en 4 axes principaux.

1. Protéger les entreprises de la Région et renforcer leur appréhension des risques cyber afin de mieux y faire face

Face à la menace cyber, protéger, sensibiliser et accompagner les entreprises est le premier et prioritaire axe de cette feuille de route cybersécurité. Il s'agit d'intervenir à deux niveaux : sensibiliser le plus grand nombre et accompagner ceux qui souhaitent aller plus loin.

1.1 Sensibiliser au risque cyber

En s'appuyant sur ses partenaires et réseaux du monde économique, l'objectif est de faire connaître aux entreprises régionales les enjeux de la cybersécurité et d'identifier celles prêtes à s'engager dans une démarche d'accompagnement.

Auprès des industriels, la Région souhaite, en parallèle à son action de développement et d'appropriation par les entreprises des briques technologiques de l'industrie 4.0, favoriser la mise en sécurité numérique des installations industrielles.

Auprès des TPE et de l'économie de proximité, elle souhaite renforcer la connaissance des bonnes pratiques d'hygiène numérique et compte s'appuyer sur des pratiques innovantes afin de renouveler les modes de communication et de pédagogie.

Enfin, il y a lieu de compléter ce travail en matière de prévention par des outils de sensibilisation des salariés et du grand public aux bonnes pratiques de sécurité numérique, ainsi que par des outils permettant le déclenchement du passage à l'action de sécurisation dans les entreprises.

Actions proposées :

- Sensibiliser les entreprises de l'économie de proximité à la cybersécurité
    - *Outils et opérations : volet sensibilisation du dispositif Atouts Numériques opéré par l'ENE Auvergne-Rhône-Alpes, portail web du Campus Région du numérique, Appel à Projet Sensibilisation à la cybersécurité dans les TPE, plan de communication-prévention, relais régional du Mois européen de la cybersécurité (en octobre) et du Cybermoi/s, sa déclinaison nationale, opérations de sensibilisation à la cybersécurité.*
- Sensibiliser les PME, en particulier industrielles
    - *Outils et opérations : plan de prévention porté par le Campus Région du numérique et décliné annuellement avec une priorisation sur un secteur d'activité, mobilisation du réseau Digitalisation des entreprises du Campus (en particulier les réseaux CCI, CMA et Auvergne-Rhône-Alpes entreprises) pour sensibiliser et former les conseillers et chargés d'affaires, promotion d'un parcours de sensibilisation spécifique « cybersécurité industrielle » au sein de l'Usine du Campus Région du numérique, développement d'une offre de découverte-formation à la gestion de crise cyber et accueil d'exercices de crise au Campus.*
- Recenser les évènements cyber et les actualités en région et les publier
    - *Outils et opérations : portail web du Campus Région du numérique, partenariats avec le réseau Digitalisation des Entreprises.*
- Soutenir des évènements dédiés à la cyber et ajouter des contenus cybersécurité aux évènements économiques et numériques sur le territoire

    - *Outils et opérations : développement d'animations pédagogiques (à l'exemple de la simulation de crise au Digital Summit 2024), soutien aux Journées de la Cyber et aux Rencontres Cybersécurité Auvergne-Rhône-Alpes, etc…*
- Sensibiliser les porteurs de projets et néo-créateurs d'entreprises aux bonnes pratiques
    - *Outils et opérations : adaptation des contenus d'accompagnement et évènements dédiés à la création-reprise*
- Mettre en place un point de contact unique d'orientation pour toutes les entreprises.
    - *Outils et opérations : étude pour identifier un modèle économique et un opérateur – il est entendu qu'il s'agit d'orientation et non pas de prise en charge, par exemple de réponse à incident.*
- Soutenir un travail de sensibilisation de la filière numérique, dont les acteurs sont en première ligne pour le conseil et la prévention dans les entreprises
    - *Outils et opérations : travail de filière via les pôles et clusters concernés.*

1.2 Accompagner les entreprises dans leurs projets cyber

La maîtrise de la gestion des risques pesant sur leurs systèmes d'information est désormais une condition indispensable pour réussir durablement la transformation numérique des entreprises.

Dès lors que les entreprises et leurs dirigeants ont pris conscience du risque cyber et souhaitent le traiter, il peut s'avérer complexe d'identifier par où commencer, sur qui s'appuyer et comment s'organiser, en particulier lorsque l'entreprise ne dispose pas de ressources humaines dédiées à son système d'information.

Une étape de diagnostic peut permettre aux dirigeants d'évaluer le niveau de sécurité du système d'information de leur entreprise, au niveau organisationnel et technique, d'identifier d'éventuelles failles de sécurité. Ensuite, l'entreprise devra se doter d'un plan pour une amélioration continue de sa cybersécurité, en identifiant et priorisant les travaux à mener pour renforcer ses infrastructures et systèmes et développer leur « cyber résilience ».

L'action régionale se donne comme objectif principal de faciliter le passage à l'action en mobilisant ses dispositifs et ses partenaires pour accompagner au plus près les entreprises souhaitant améliorer leur cybersécurité.

<u>Actions proposées :</u>

- Accompagner financièrement l'intervention d'experts cybersécurité dans les entreprises
    - *Outils et opérations : volet numérique du dispositif Industrie du Futur (industrie et services à l'industrie), accompagnements Atouts numériques (TPE, entreprises de l'économie de proximité), EDIH Minasmart, prestations d'accompagnement des plateformes de l'Usine du Campus, aides au diagnostic cyber pour les PME hors industrie.*
- Sécuriser les projets innovants afin de les prémunir contre le vol de données, l'espionnage industriel et la cybermalveillance
    - *Outils et opérations : incitation au « security by design » pour les projets d'innovation soutenus par la Région, attention accordée dans l'analyse aux politiques de cybersécurité des projets, accompagnements par Minalogic.*
- Investir dans un outil de simulation permettant la démonstration et le test des solutions cyber
    - *Outils et opération : installation d'un simulateur « IT/OT » au Campus Région du numérique.*
- Améliorer la performance cyber des prestataires numériques au bénéfice de leurs clients
    - *Outils et opérations : accompagnement à la certification ISO 27001 en s'appuyant sur l'expertise de Digital League, étude en partenariat avec la filière cyber des leviers d'incitation, de formation, de certification, de labellisation pour favoriser une plus forte culture cyber auprès des prestataires numériques*
- Favoriser les retours d'expérience et accompagner les responsables de Systèmes d'Information attaqués

    - *Outils et opérations : soutien à la création d'un espace d'échange pour les spécialistes et/ou les dirigeants ayant subi des cyberattaque, fonctionnant sous la règle de Chatham House.*
- Partager le module 17cyber permettant aux victimes d'actes de cybermalveillance de réaliser un diagnostic en ligne et de bénéficier de conseils personnalisés.
    - *Outils et opérations : intégration du module créé par Cybermalveillance.gouv.fr au sein du portail web Campus Région du numérique.*

2. Animer et développer la filière cybersécurité régionale

La filière cybersécurité inclut « côté demande » des spécialistes de la sécurité des systèmes d'information ou des généralistes prenant en compte la thématique de la sécurité numérique et « côté offre » des entreprises proposant des solutions, des produits ou services uniquement dédiés à la cybersécurité ou associant de telles propositions à une offre de service généraliste.

Différents réseaux coexistent à ce jour, au niveau régional et national, pour fédérer ces opérateurs. Il s'agit donc dans un premier temps de prolonger et amplifier l'effort pour réunir, mobiliser et animer le plus d'acteurs régionaux de la cybersécurité, de leur offrir des opportunités de visibilité pour favoriser leur développement et de s'attacher à favoriser l'innovation en leur sein.

2.1 Réunir, mobiliser et animer

Afin de renforcer l'efficacité de son action en matière de cybersécurité, il est primordial pour la Région de réunir, de mobiliser et d'animer les acteurs de son écosystème régional dans une **logique de coordination**. Une approche pragmatique sera privilégiée par la mobilisation des énergies existantes autour d'objectifs communs, **sans recourir à la création de nouvelles structures**. Il s'agit donc de s'appuyer sur l'écosystème en place et ses acteurs pour mutualiser et optimiser les efforts et les ressources, en renforçant les liens entre les différents intervenants. L'objectif est de **créer une dynamique collective** où chacun contribue, selon son expertise, à l'amélioration de la sécurité numérique de son territoire.

Actions proposées :

- Soutenir les réseaux de professionnels pour favoriser les échanges et la collaboration.
    - *Outils et opérations : soutien au cluster du numérique dans ses actions cyber (club experts, évènements…).*
- Mutualiser les actions des acteurs de l'écosystème
    - *Outils et opérations : mise à disposition de moyens du Campus Région du numérique pour, par exemple, coordonner des plannings, coproduire des évènements ou des livrables en commun (études, guides pratiques…).*
- Maintenir à jour une vision claire et exhaustive du paysage de la cybersécurité et de l'offre régionale, afin de faciliter la mise en relation entre les besoins et les solutions
    - *Outils et opérations : panorama de la cybersécurité par la plateforme IET (Intelligence Economique et Territoriale) de l'agence Auvergne-Rhône-Alpes entreprises, référencement et cartographie des entreprises expertes en cybersécurité.*

2.2 Mettre en visibilité et promouvoir les offreurs de solution régionaux

Favoriser le développement d'une filière régionale forte et compétitive implique d'abord de mettre en lumière et de promouvoir les prestataires régionaux et leur savoir-faire. Pour ce faire, la Région

souhaite soutenir des actions concrètes pour qualifier, segmenter et diffuser l'offre régionale de solutions cyber.

Il s'agit d'encourager une « préférence numérique régionale » et de favoriser les solutions souveraines, en tenant compte des besoins et des niveaux de maturité des différentes organisations.

En parallèle, il apparait important d'assurer une présence forte de la Région sur les événements de référence en France et à l'international, afin de soutenir le développement de nos entreprises sur ces marchés.

Prioritairement, et en continuité parfaite avec la stratégie régionale de soutien à l'industrie, c'est une valorisation de l'expertise en matière de cybersécurité industrielle qui sera recherchée.

Actions proposées :

- Qualifier et segmenter l'offre cyber selon les besoins et les niveaux de maturité
    - *Outils et opérations : développer une plateforme en ligne pour présenter les solutions de cybersécurité régionales, au-delà du référencement et de la cartographie prévus plus haut dans un effort de cohérence des propositions selon des parcours orientés besoins.*
- Assurer la présence de la Région Auvergne-Rhône-Alpes sur des évènements de référence
    - *Outils et opérations : politique évènementielle de filières (exemples : Forum In Cyber à Lille, Lyon Cyber Expo) incluant des Appels à Manifestation d'Intérêt pour accompagner sur ces salons des entreprises régionales.*
- Soutenir le développement des entreprises régionales en France et à l'international
    - *Outils et opérations : plans de développement international proposés par les Pôles et Clusters.*

2.3 Favoriser l'investissement, la recherche et l'innovation

Dans l'objectif de faire d'Auvergne-Rhône-Alpes une terre d'innovation en matière de cybersécurité, notamment de cybersécurité industrielle, la Région souhaite voir émerger sur le territoire de nouvelles entreprises, futures pépites de l'écosystème cyber. Pour cela, la Région souhaite favoriser l'incubation et le développement de start-up. Des partenariats avec les spécialistes de l'écosystème tech (incubateurs, accélérateurs) et des fonds d'investissement seront recherchés à cette fin.

Il est, par ailleurs, entendu que l'outil prioritaire pour favoriser l'innovation et travailler au rapprochement du monde de la recherche avec les entreprises est le Pôle de Compétitivité.

Actions proposées :

- Soutenir les efforts des acteurs de l'écosystème en faveur de la recherche et de l'innovation
    - *Outils et opérations : soutien au Pôle de compétitivité dans ses actions cyber, renforcement des liens avec les incubateurs, accélérateurs et starts-ups studios spécialisés.*
- Veiller à ouvrir aux activités de recherche le centre cyber du Campus Région du numérique
    - *Outils et opérations : utiliser le simulateur « IT/OT » et les espaces cyber du Campus à des fins de recherche et d'innovation.*
- Mobiliser les dispositifs régionaux en complément des opportunités nationales et européennes pour financer les projets d'innovation
    - *Outils et opérations : faire connaitre les dispositifs régionaux existants (partenariats d'innovation R&D booster, I DEMO…) et organiser un évènement de valorisation des sujets de recherche auprès des entreprises de la filière.*

3. Développer les compétences en matière de cybersécurité

Le domaine de la cybersécurité est unanimement identifié comme un secteur d'avenir, porteur en termes d'emploi et offrant des débouchés professionnels variés.

Parallèlement, la filière d'un côté, les entreprises et collectivités de l'autre, font face à un **déficit de main d'œuvre** alors qu'ils ont besoin de pourvoir des postes de tous niveaux de diplômes et pour des domaines variés : programmation, réseau, commercial, juridique… On estime que plus de 15000 postes en cybersécurité sont disponibles et non couverts en France (données étude Wavestone 2023).

Le développement de la filière cybersécurité, au même titre que le secteur numérique dans son ensemble, nécessite la formation de talents rares, leur captation et leur rétention. Leur disponibilité est un facteur important pour le développement du tissu économique régional, sa capacité d'innovation mais aussi pour l'attractivité du territoire.

Il est donc proposé d'agir en amont sur l'attractivité des métiers de la cybersécurité, en particulier auprès des **jeunes en questionnement d'orientation et de leurs parents** ainsi qu'auprès des **femmes**, afin de favoriser la mixité, et des **publics en reconversion**. Assurer ainsi un vivier de candidats élargi conforte l'excellence de l'offre de formation et permet d'augmenter le volume de diplômés experts, spécialistes et/ou acculturés à la cybersécurité.

3.1 Promouvoir les métiers / susciter des vocations

Rendre la filière et ses métiers attractifs constitue un effort de moyen et long terme afin d'augmenter le nombre de candidats potentiels pour les formations initiales spécialisées en cybersécurité.

Il est impératif de renforcer l'attractivité des métiers de la cybersécurité et de susciter des vocations chez les jeunes et les professionnels en reconversion. La filière, en constante évolution, a besoin de talents variés et compétents pour assurer la sécurité numérique de notre société et de notre économie. Pour atteindre cet objectif, la Région doit agir sur plusieurs leviers clés, notamment la promotion des métiers, la valorisation des compétences et l'encouragement de la diversité au sein de la filière.

Actions proposées :

- Soutenir des concours et compétitions de piratage éthique et de cybersécurité permettant aux jeunes talents de se mesurer et de se former de manière ludique
    - *Outils et opérations : soutenir l'organisation du CSAW à Valence (finale européenne de cette compétition mondiale de cybersécurité), appuyer d'autres évènements similaires sur le territoire régional, faire émerger une compétition de référence en Auvergne-Rhône-Alpes et soutenir une équipe régionale pour faire (re)connaître l'excellence régionale en cybersécurité.*
- Mener et soutenir des actions de valorisation des métiers de la filière
    - *Outils et opérations : mobiliser le portail web du Campus Région du numérique, imaginer un stand dédié au Mondial des Métiers, mettre en place des actions de valorisation avec Auvergne-Rhône-Alpes Orientation.*
- Promouvoir l'emploi féminin
    - *Outils et opérations : relais de campagne de promotion, veiller à la représentativité des métiers de la cyber dans les opérations dédiées à la mixité dans le numérique, valoriser des role-models féminins dans les évènements.*

3.2 Développer l'offre de formation

La formation représente un axe important d'une stratégie au service de la sécurité numérique des acteurs régionaux sur deux versants :

- Afin de répondre à la très forte demande en compétences du secteur et soutenir sa croissance : il s'agit de former davantage de personnes aux métiers de la cybersécurité incluant toutes les déclinaisons de niveau de spécialisation, du technicien à l'expert de haut niveau, en formation initiale et continue.
- Afin d'élever le niveau de sécurité global et de soutenir la demande : il s'agit de former le plus grand nombre de dirigeants et de salariés aux enjeux, dangers et bonnes pratiques de la cybersécurité.

Pour le premier versant, la Région Auvergne-Rhône-Alpes souhaite encourager la croissance du nombre de spécialistes formés aux métiers de la cybersécurité. Il est rappelé d'ailleurs qu'il ne s'agit pas exclusivement de métiers techniques mais aussi des activités relevant du droit, de la qualité ou encore de la communication.

Pour le second versant, les actions de sensibilisation vers les entreprises figurant plus haut (au 1.1) ont vocation à favoriser l'appétence des entreprises pour proposer à leurs équipes des actions de sensibilisation et de formation de leurs collaborateurs.

Actions proposées :

- Compléter et actualiser la connaissance et la vision de l'offre de formation, dans une logique prospective
    - *Outils et opérations : cartographie et qualification des formations disponibles, lancement d'une étude transversale sur les besoins en compétences à moyen terme (dans les entreprises et les prestataires de la filière) et les viviers disponibles (formation initiale, continue, reconversions...).*
- Favoriser des reconversions et des montées en compétence en formant les demandeurs d'emploi aux fonctions cyber
    - *Outils et opérations : marchés de services de formation professionnelle au bénéfice des demandeurs d'emploi.*
- Financer des investissements pédagogiques en cyber pour encourager la création de modules et programmes de formation spécialisés en cybersécurité dans les établissements d'enseignement supérieur
    - *Outils et opérations : appel à projet annuel « Agir pour la réussite étudiante » et plan régional « Région des Ingénieurs et des Techniciens ».*
- Doter le Campus Région du numérique d'un « lab » de formation à la cybersécurité
    - *Outils et opérations : création d'une salle de TP cybersécurité associée à un simulateur, création d'un espace dédié à l'investigation cyber (« lab forensics ») et d'une salle de gestion de crise. Développement d'une offre de formation continue à la gestion de crise.*
- Fédérer les écoles et organismes de formation proposant des cursus cybersécurité en Auvergne-Rhône-Alpes
    - *Outils et opérations : mobilisation et éventuelles adaptations du Label Campus région du numérique et du Club Ecole coanimé par le Campus et Digital League afin de mener des actions spécifiques sur la thématique de la cybersécurité.*

4. Mettre en place une gouvernance régionale adaptée de la thématique

Afin d'ancrer Auvergne-Rhône-Alpes comme « région du numérique » tout en étant réaliste sur les moyens disponibles, il est proposé avant tout de capitaliser sur les investissements récents et prévus sur le Campus Région du numérique. L'infrastructure qui s'agrandira au printemps 2025 peut être mobilisée pour constituer le centre névralgique de la cybersécurité régionale. Mais en parallèle, maintenir une forte dynamique collective sera un facteur-clé de succès afin de

coordonner et relayer avec le plus d'efficience possible l'ensemble des initiatives émergeant dans la Région.

4.1 Faire du Campus Région du numérique un lieu totem de la cyber

Le site de Charbonnières-les-Bains, accueillant depuis 2021 le projet emblématique de Campus Région du numérique, constitue la base idéale pour en faire le lieu totem de la cybersécurité pour Auvergne-Rhône-Alpes. **Faire du Campus Région du numérique un centre d'excellence pour la cybersécurité constituera donc l'axe majeur** de la politique régionale.

A date, en 2025, 5 programmes de formation en cybersécurité sont d'ores et déjà établis au Campus Région du numérique :

- Administrateur d'Infrastructures Sécurisées (M2i Formation)
- Responsable Cybersécurité (CSB School)
- Spécialiste Cybersécurité (CSB School)
- Consultant expert en cybersécurité (IT-Akademy)
- Manager de la cybersécurité industrielle (Mines St Etienne)

5 structures d'accompagnement (pôles et clusters, associations et consortias de l'Usine) y proposent des parcours de sensibilisation et des accompagnements autour de la cybersécurité, en particulier industrielle, ou s'attachent à fédérer les entreprises de la filière numérique :

- SWARM
- DIWII
- Digital League
- ENE
- Minalogic

Plusieurs entreprises spécialisées complètent ce panorama des résidents du Campus et démontrent la centralité du Campus Région du numérique pour adresser la thématique de la cybersécurité. Pour aller plus loin, il s'agit d'abord d'accueillir au sein des espaces du Campus de nouveaux **événements** orientés sensibilisation ou des conférences de haut niveau sur la cybersécurité. Pour favoriser ces évènements, des partenariats entre le Campus et les organisateurs pourront être recherchés.

Des écoles, des entreprises et des acteurs institutionnels du numérique travaillant sur la cybersécurité sont déjà résidents du Campus Région du numérique : **l'accueil de nouveaux acteurs** de la filière cybersécurité sera recherché afin d'amplifier les synergies et les partenariats.

Avec la mise en œuvre sous maîtrise d'ouvrage régionale d'actions autour de la sensibilisation, de l'innovation et de la formation, figurant dans les axes de la présente feuille de route, **la labellisation Campus Cyber territorial** peut constituer pour le Campus Région du numérique un objectif à moyen terme. La Région est attachée à l'émergence d'une solution adaptée aux besoins du territoire et cette labellisation ne constitue qu'un moyen supplémentaire de rayonnement de l'expertise cyber d'Auvergne-Rhône-Alpes. Aussi, l'émergence d'une structure juridique autonome associée à un modèle économique solide n'est pas, par principe, écartée. Il est important en revanche de bien veiller à conserver la dynamique collective.

Actions proposées :

- Faire du Campus Région du numérique un centre d'excellence cyber
    - *Outils et opérations : accueil d'entreprises et de nouveaux opérateurs de formation, plus de 800m2 dédiés à la cybersécurité, incluant les investissements dédiés à la formation prévus plus haut, accueil d'évènements.*
- Insérer le Campus Région du numérique dans les dynamiques nationales et européennes
    - *Outils et opérations : adhésion au Campus Cyber, coopérations avec l'ANSSI et Cybermalveillance.gouv.fr, échanges avec les autres Campus territoriaux, réflexion autour d'une éventuelle labellisation nationale « Campus Cyber Auvergne-Rhône-Alpes ».*
- Animer une coordination des résidents du Campus Région du numérique intervenants en cyber
    - *Outils et opérations : comité technique cyber des membres du Campus dédié à la conduite de projets mutualisés autour de la cybersécurité, en particulier industrielle.*

4.2 Favoriser une gouvernance collective

A l'issue du travail de concertation et de coordination mené en 2024 autour du Campus Région du numérique, une dynamique collective a été renforcée et la Région souhaite la maintenir et la développer.

Par ailleurs, pour guider son action, la Région souhaite mettre en place une **gouvernance régionale de la thématique.** Cette instance pourrait être un espace de concertation autour de l'animation globale et permettrait de formaliser des objectifs stratégiques, ainsi que de consolider un programme d'animation régional maillant le territoire.

Enfin, cette logique de large coopération permettra de travailler collectivement sur deux idées au service du territoire : l'élaboration d'un **baromètre cyber régional** et la **constitution d'un collectif** de bénévoles mobilisables sur diverses actions collectives ou individuelles.

Actions proposées :

- Créer une « Team Cyber Auvergne-Rhône-Alpes » composée de Minalogic, Digital League, l'ENE Auvergne Rhône-Alpes, l'ADIRA, le Clusir et l'agence Auvergne Rhône-Alpes entreprises, et les réunir sous une charte commune
    - *Outils et opérations : définition d'une identité commune et co-écriture d'une charte de coordination*
- Regrouper les acteurs régionaux (services de l'Etat et institutionnels, entreprises de la filière, monde économique, spécialistes cyber des DSI, représentants du monde académique et de la formation, de la recherche et de l'innovation) dans un comité de pilotage cyber régional
    - *Outils et opérations : mobilisation des structures existantes pour constituer les différents « piliers » de cette gouvernance, réunion annuelle de ces membres*
- Coordonner un baromètre cyber régional
    - *Outils et opérations : collecte de données à un échelon régional, recherche de données manquantes et publication annuelle d'une synthèse permettant d'évaluer et orienter les actions.*
- Impulser une « réserve cyber Auvergne-Rhône-Alpes »
    - *Outils et opérations : animation d'un collectif de spécialistes cyber, volontaires pour mener des actions de sensibilisation, de découverte des métiers (conférences, salons de l'orientation…), d'appui à des pairs en difficultés ou de premier niveau de conseil à des organisations.*

Mise en œuvre, suivi et évaluation

Animation de la démarche

Afin d'adapter la thématique d'une part aux enjeux, évoluant sans cesse, mais aussi à l'écosystème et sa structuration ainsi qu'aux moyens de la collectivité, il est proposé de définir annuellement un plan d'action cybersécurité.

Le Campus Région du numérique, direction de la Région rattachée à la DGA Economie, Formation, Enseignement Supérieur, Innovation, Tourisme, est chargé d'animer en transversalité avec les services concernés la Feuille de Route Cybersécurité et d'en rendre compte annuellement à la Commission Economie, Relocalisations, Numérique et Préférence régionale

En lien avec les différentes structures intervenantes, comme évoqué au 4.2 de la présente, une gouvernance collective permettant d'orienter les actions et de gérer collégialement la thématique à l'échelle régionale, sera mise en place. Elle pourra donner lieu par exemple chaque année à des assises régionales de la cybersécurité.

Dans cette perspective, la Région entend prolonger et amplifier le travail partenarial, en associant notamment les services de l'Etat en charge (ANSSI, Cybermalveillance.gouv.fr, DREETS, forces de l'ordre…) et le réseau Digitalisation des Entreprises du Campus (constitué notamment par les CCI d'Auvergne-Rhône-Alpes, la Chambre des Métiers et de l'Artisanat, l'agence Auvergne-Rhône-Alpes Entreprises, le MEDEF et la CPME). Plus localement, pour mener les sujets cyber au sein du Campus Région du numérique, l'ensemble de ses résidents seront associés.

Suivi et évaluation

Un baromètre régional de la cybersécurité intégrera les éléments clés nécessaires à une photographie précise des réalités régionales et constituera un ensemble d'indicateurs clés. Seront notamment suivis annuellement :

- Le nombre d'entreprises sensibilisées
- Le nombre de nouveaux diplômés spécialistes en cybersécurité

Il s'attachera également à évaluer les volumes de cyberattaques dans la région, la prise de conscience des risques cyber dans les entreprises et leur degré de préparation, ainsi que les retombées économiques négatives (conséquence de la cybercriminalité) et positives (le développement de la filière cyber et des entreprises du numériques spécialisées).

Ressources mises en œuvre

Au sein du Campus Région du numérique, le pilotage des actions ainsi que la coordination de la thématique en transversalité sera assurée par l'équipe technique en place. A l'issue de la période de montée en puissance, estimée à une année, un bilan des ressources mobilisées et à mobiliser sera réalisé.

Toujours dans une optique de réalisme et de pragmatisme, la thématique de la cybersécurité fera l'objet d'une animation transversale et cette nouvelle politique régionale n'aura pas d'impact budgétaire en tant que tel : chaque direction et programme inclura autant que de besoin la thématique dans son action. L'effort principal nouveau est porté en fonctionnement comme en investissement par le Campus Région du numérique.

La recherche d’opportunités de financement, notamment européens, et de synergies avec les opérateurs publics de la cybersécurité sera permanente afin de maximiser l’impact des actions au bénéfice des entreprises de la région Auvergne-Rhône-Alpes.